(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年2 月5 日 (05.02.2004)

PCT

(10) 国際公開番号
WO 2004/011746 A1

(51) 国際特許分類[7]: E05B 49/00, G08B 25/04

(21) 国際出願番号: PCT/JP2003/009755

(22) 国際出願日: 2003 年7 月31 日 (31.07.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-223700 2002 年7 月31 日 (31.07.2002) JP
特願2002-278436 2002 年9 月25 日 (25.09.2002) JP
特願 2002-298309
2002 年10 月11 日 (11.10.2002) JP
特願 2002-302996
2002 年10 月17 日 (17.10.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川6丁目7番35号 Tokyo (JP).

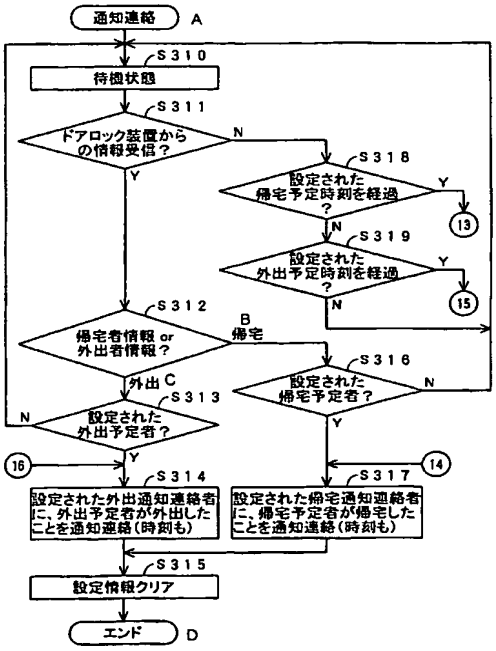
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 油井 康二 (YUI,Yasuji) [JP/JP]; 〒141-0001 東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 松村 広幸 (MATSUMURA,Hiroyuki) [JP/JP]; 〒141-0001 東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 八重樫 章 (YAEGASHI,Akira) [JP/JP]; 〒141-0001 東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 中村 友之 (NAKAMURA,Tomoyuki); 〒105-0001 東京都 港区 虎ノ門1丁目2番3号 虎ノ門第一ビル9階 三好内外国特許事務所内 Tokyo (JP).

[続葉有]

(54) Title: COMMUNICATION DEVICE

(54) 発明の名称: 通信装置



A...NOTIFY
S310...STANDBY STATE
S311...INFORMATION RECEIVED FROM DOOR LOCK DEVICE?
S318...SCHEDULED ARRIVAL TIME PASSED?
S319...SCHEDULED DEPARTURE TIME PASSED?
S312...INFORMATION OF ARRIVING PERSON OR DEPARTING PERSON?
B...ARRIVAL
C...DEPARTURE
S316...PERSON SCHEDULED TO ARRIVE
S313...PERSON SCHEDULED TO DEPART
S314...NOTIFY PERSON, WHO IS DESIGNATED TO BE NOTIFIED OF DEPARTURE, THAT PERSON SCHEDULED TO DEPART HAS DEPARTED (AND TIME AS WELL)
S317...NOTIFY PERSON, WHO IS DESIGNATED TO BE NOTIFIED OF ARRIVAL, THAT PERSON SCHEDULED TO ARRIVE HAS ARRIVED (AND TIME AS WELL)
S315...CLEAR ESTABLISHED INFORMATION
D...END

(57) Abstract: A communication device that can urge a person who has gone out, for example, a child to come home when it is a scheduled time to do so, and that can notify, for example, his or her parent of a time when he or she will come home. There is provided door lock control means that uses first communication means to communicate with an electronic key device storing at least electronic key information, and that compares received electronic key information with the electronic key information stored in a memory part to control, based on a result of the comparison, the lock mechanism of the door. There is also provided user-identifying means that identifies, based

[続葉有]

WO 2004/011746 A1

(81) 指定国 (国内): CN, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

on information received from the electronic key device via the first communication means, the user of the electronic key device. Transmission control means causes, based on a result of identification made by the user identifying means, information concerning arrival and departure of the user of the electronic key device to be transmitted to a predetermined destination via second communication means.

(57) 要約: 外出していたもの、例えば子供に帰宅予定時刻になったときに帰宅を促すことができると共に、当該子供の帰宅時刻を、例えば親にも通知連絡することができるようにした通信装置を提供する。第１の通信手段により、少なくとも電子鍵情報を記憶する電子鍵装置と通信を行ない、受信した電子鍵情報と、記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいてドアのロック機構を制御するドアロック制御手段を備える。また、第１の通信手段を通じて電子鍵装置から受信した情報に基づいて電子鍵装置の使用者を認識する使用者認識手段を設ける。送信制御手段は、使用者認識手段での認識結果に基づいて、電子鍵装置の使用者の入退出に関する情報を、予め定められている通知先に第２の通信手段を介して送信するように制御する。

明　細　書

通信装置

技術分野

この発明は、電子鍵情報を用いてドアの施錠、開錠を制御するようにするドアロック制御システムに用いて好適な通信装置に関する。

背景技術

最近、従来の物理的な鍵を鍵シリンダーに差し込んで施錠、開錠を行なうドアロック制御システムを玄関ドアなどに採用している住戸等においては、鍵シリンダー機構に精通しているものが、鍵を用いずに開錠することによる盗難等の事件が発生している。

そこで、このような鍵シリンダー機構を用いない電子鍵装置によるドアロック制御システムが注目されている。例えば、この電子鍵装置によるドアロックシステムの一例として、親機は、予め登録されている電子鍵情報としてのＩＤコードと、電子鍵情報としての子機から受信したＩＤコードを比較照合して、その比較結果に基づいてドアロックをコントロールするものが知られている（例えば特許文献１（特開平９－４２９３号公報参照））。

例えば、外出した子供に、所定の時刻までに帰宅するように約束させた場合であっても、子供はその時刻を失念してしまうことはよくある。この場合に、家に親がいれば、子供が約束の時刻に帰宅していない場合には、親が子供の携帯電話端末などに電話をかけることにより帰宅を促すことができる。

しかし、親が共に仕事等で外出していて留守にしている場合、子供が所定の時刻に帰宅したかどうかを確認することできない。そのため、子供に帰宅を促すことができない。

子供に、帰宅時に親に電話させるなどの方法により帰宅を知らせるようにすることも考えられる。しかしながら、電話により帰宅の連絡を受けたとしても、本当に帰宅したかどうかを確認することはできない。

この発明は、上述の点にかんがみ、外出していたもの、例えば子供に帰宅予定時刻になったときに帰宅を促すことができると共に、当該子供の帰宅時刻を、例えば親にも通知連絡することができるようにした通信装置を提供することを目的とする。

発明の開示

上記課題を解決するために、請求項１の発明による通信装置は、少なくとも電子鍵情報を記憶する電子鍵装置と通信を行なう第１の通信手段と、通信ネットワークを通じて情報送信を行なうための第２の通信手段と、電子鍵情報を記憶する記憶部と、前記第１の通信手段を通じて前記電子鍵装置から受信する電子鍵情報と、前記記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいてドアのロック機構を制御するドアロック制御手段と、前記第１の通信手段を通じて前記電子鍵装置から受信した情報に基づいて当該電子鍵装置の使用者を認識する使用者認識手段と、前記使用者認識手段での認識結果に基づいて、前記電子鍵装置の使用者の入退出に関する情報を、予め定められている通知先に前記第２の通信手段を介して送信するように制御する送信制御手段と、を備えることを特徴とする。

また、請求項２の発明は、請求項１に記載の通信装置において、前記通知先に入退出に関する情報を送信すべき前記電子鍵装置の使用者の設

定を受け付けて記憶する設定記憶手段を備え、前記送信制御手段は、前記設定された前記電子鍵装置の使用者の入退出に関する情報を、前記第２の通信手段を介して前記通知先に送信することを特徴とする。

この発明による通信装置においては、使用者認識手段は、電子鍵装置と通信を行なってドアの開閉をした者が誰であるかを認識する。送信制御手段は、予め設定された通知先に電子鍵装置の使用者の入退出に関する情報を送信する。

したがって、例えば通知先を外出している親としておくことにより、例えば子供の帰宅や外出に関する情報を親に通知することができる。

また、請求項３の発明は、請求項２に記載の通信装置において、前記設定記憶手段では、前記電子鍵装置の使用者と共に、当該使用者に対応して時刻情報の設定入力を受け付けて記憶し、前記送信制御手段は、前記設定入力された時刻情報に対応する時刻を経過しても、前記使用者認識手段で前記設定された前記電子鍵装置の使用者を認識しなかったときに、当該電子鍵装置の使用者の入退出がなされていないことに関する情報を、前記通知先に前記第２の通信手段を介して送信するように制御することを特徴とする。

請求項３の発明においては、例えば帰宅予定時刻を設定しておくと共に、通報先を帰宅予定者と設定することにより、設定された時刻を経過しても帰宅予定者が帰宅していないときには、当該帰宅予定者にその旨を通知することができる。また、通報先として帰宅予定者以外の者、例えば親に設定しておけば、親に帰宅予定者が帰宅していないことを通知することができる。

図面の簡単な説明

図１は、この発明のドアロック制御システムの実施の形態で用いる識

別情報の概要を説明するための図である。

図２は、この発明の実施形態で用いる識別情報の一例を示す図である。

図３は、この発明によるドアロック制御システムの実施形態が適用された通信システムの概要を説明するための図である。

図４Ａおよび図４Ｂは、この発明による電子鍵装置の一実施形態を示す図である。

図５は、この発明による電子鍵装置の一実施形態の構成例を示すブロック図である。

図６は、この発明による電子鍵装置の一実施形態の動作を説明するためのフローチャートである。

図７Ａおよび図７Ｂは、この発明による電子鍵装置の他の実施形態を示す図である。

図８は、この発明による電子鍵装置の他の実施形態の構成例を示すブロック図である。

図９は、この発明による電子鍵装置の他の実施形態の動作を説明するためのフローチャートである。

図１０Ａおよび図１０Ｂは、実施形態のドアロック制御システムを構成するドアロック装置の一例の要部を説明するための図である。

図１１は、図１０Ａおよび図１０Ｂのドアロック装置のドアロック制御装置の構成例を示すブロック図である。

図１２は、セキュリティシステムに用いる監視制御装置の例を示す図である。

図１３は、図１２の監視制御装置の構成例を示すブロック図である。

図１４は、個人プロファイル情報の一例を示す図である。

図１５は、セキュリティモードの内容を説明するための図である。

図１６は、セキュリティモードの内容を説明するための図である。

図１７は、管理サーバ装置の構成例を示すブロック図である。

図１８は、図１２の監視制御装置の伝言記録および再生機能を説明するためのフローチャートである。

図１９は、ドアロック制御モードの設定動作を説明するためのフローチャートである。

図２０は、ドアロック制御モードの設定動作を説明するためのフローチャートである。

図２１は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図２２は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図２３は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図２４は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図２５は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図２６は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図２７は、ドアロック制御モードの一つの例である逐次ロックモード

でのドアロック制御動作を説明するためのフローチャートの一部である。

図２８は、ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図２９は、ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図３０は、監視制御装置のリモートコマンダからの信号の受信処理動作を説明するためのフローチャートである。

図３１は、監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

図３２は、監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

図３３は、監視制御装置におけるドアロック装置との連携動作を説明するための図である。

図３４は、この発明における実施形態において、本鍵情報の登録を説明するためのフローチャートを示す図である。

図３５は、この発明における実施形態において、本鍵情報の登録を説明するためのシステム構成を示す図である。

図３６は、この発明における実施形態において、帰宅予定あるいは外出予定の設定処理を説明するためのフローチャートの一部を示す図である。

図３７は、この発明における実施形態において、帰宅予定あるいは外出予定の設定処理を説明するためのフローチャートの一部を示す図である。

図３８は、この発明における実施形態において、帰宅予定者あるいは外出予定者に関する通知連絡処理を説明するためのフローチャートの一部を示す図である。

図３９は、この発明における実施形態において、帰宅予定者あるいは外出予定者に関する通知連絡処理を説明するためのフローチャートの一部を示す図である。

図４０は、この発明における実施形態において、帰宅予定者あるいは外出予定者に関する通知連絡処理を説明するためのフローチャートの一部を示す図である。

発明を実施するための最良の形態

以下、この発明による通信装置の実施形態を含む通信システムを、図を参照しながら説明する。

以下に説明する通信システムでは、家の玄関ドアに、電子鍵装置と電子鍵情報の通信を行なって施錠、開錠を制御するようにするドアロック制御システムを設ける。また、この例では、家の中には、窓や玄関ドアからの賊の侵入、火災の発生、ガス漏れを検知して、それぞれの異常事態に対応する措置を取るセキュリティ監視システムを設け、このセキュリティ監視システムとドアロック制御システムとを、通信可能に接続して連動させて動作させるようにしている。

そして、さらに、この例では、セキュリティ監視システムは、通信ネットワークを通じて管理サーバ装置に接続して、全体として、通信システムを構成している。

そして、この例においては、ドアロック制御システムを構成する後述のドアロック装置と、セキュリティ監視システムを構成する後述の監視制御装置とにより、この実施形態の通信装置を構成している。

また、この実施形態においては、電子鍵装置は、生体情報取得部と、制御用ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）と、通信手段とを備えるもので、種々の形態のものが使用可能である。この例では、こ

の電子鍵装置の具体例としては、ＩＣカードの他、携帯電話端末、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）端末などを用いることもできる。

電子鍵装置に搭載される制御用ＩＣは電子鍵情報用メモリを備え、その電子鍵情報用メモリには、電子鍵情報が格納されている。この電子鍵情報としては、この例では、同一のものが存在しないように一元管理された識別情報が記憶される。この例では、この識別情報としては、ＩＣチップ製造番号が用いられる。

例えば、図１に示すように、１社あるいは複数社のＩＣチップの製造会社１００１において、製造した制御用ＩＣチップ１００２に対して、一元管理された重複のないＩＣチップ製造番号を付与するようにする。ＩＣチップの製造会社１００１が複数社の場合には、例えば、それぞれのＩＣチップ製造会社１００１に、予め、制御用ＩＣチップ１００２に付与する製造番号を割り当てておくようにすることにより、一元管理される。したがって、製造された制御用ＩＣチップ１００２のメモリには、互いに異なるＩＣチップ製造番号が識別情報として記憶される。

この制御用ＩＣチップ１００２は、ＩＣカード製造工場（あるいは製造会社）１００３、携帯電話端末製造工場（あるいは製造会社）１００４、ＰＤＡ端末製造工場（あるいは製造会社）１００５などに供給されて、それらの制御用ＩＣチップと通信手段とが搭載されたＩＣカード、携帯電話端末、ＰＤＡ端末などが製造される。

図２は、この実施形態で用いられるＩＣチップ製造番号の一例を説明するための図である。

この例のＩＣチップ製造番号は、３桁のメーカー番号と、３桁のカテゴリーコードと、４桁のシリアル番号とからなる、合計１０桁の番号（記号を含む）で構成される。

なお、識別情報は、ＩＣチップ製造番号の限定されるものではなく、同一のものが存在しないように一元管理された情報であれば、どのようなものも使用可能である。また、識別情報は、ＩＣチップ製造番号と共に、別個にＩＣのメモリに記憶するようにしてもよい。

電子鍵装置の通信手段としては、この例では、電磁誘導や電波を用いた非接触による通信手段が用いられる。この実施形態においては、この通信手段は、例えば数ミリメートル～数十センチメートルの範囲で通信ができるものであればよく、小パワーのもので十分である。

次に、この実施形態におけるドアロック制御システムにおいては、玄関ドアには、電子鍵装置によりドアの施錠、開錠を行なえるようにするためのドアロック装置が取り付けられる。この例では、電子鍵装置とドアロック装置との間では、電子鍵情報の通信を行ない、ドアロック装置は、その通信に基づいてドアの施錠、開錠を制御するようにする。

以下に説明する例では、電子鍵装置とドアロック装置との間の通信は、電磁誘導を用いた非接触による通信とされており、後述するように、ドアロック装置の一部を構成する電子鍵装置のリード／ライト部を介して、通信が行われる。

この実施形態では、ドアの施錠、開錠を制御するための電子鍵情報としては、前述したＩＣチップ製造番号からなる識別情報が用いられる。この実施形態では、当該家における電子鍵情報として、前述のようにして一元管理された識別情報が内蔵メモリに書き込まれた電子鍵装置の前記識別情報を電子鍵情報として管理サーバ装置に登録することにより、家族構成員のそれぞれが、自分用の電子鍵装置を所有して使用するようにする。

この実施の形態では、管理サーバ装置は、登録された家族構成員のそれぞれについての電子鍵情報をドアロック装置の電子鍵情報の記憶部に

転送して、電子鍵情報をドアロック装置に登録させるようにする。ドアロック装置は、登録された電子鍵情報と、通信装置としての電子鍵装置から受信した電子鍵情報とを比較し認証して、その結果に応じてドアの施錠、開錠を制御する。

後述するように、この実施形態では、家族構成員のそれぞれは、自分用の電子鍵情報として、本鍵情報と、バックアップ鍵情報とを管理サーバ装置に登録することができる。電子鍵情報は、前述したように、電子鍵装置ごとに異なるので、本鍵情報とバックアップ鍵情報との登録は、本鍵装置と、バックアップ鍵装置との登録に等しい。

以下に説明する例においては、各人に与えられる本鍵装置としては、ドアロック制御システムの提供会社が提供するＩＣカードとされる。そして、この本鍵装置であるＩＣカードの識別情報が、ドアロック制御システムが当該家に取り付けられる前に、予め管理サーバ装置に、当該ＩＣカードの所有者の電子鍵情報として登録される。

この場合に、この実施形態では、家族構成員の数分だけ、ＩＣカードが前記提供会社から提供され、それらの複数のＩＣカードの全ての識別情報が、設置されるドアロック制御システム用の電子鍵情報として管理サーバ装置に登録される。

さらに、この実施形態では、管理サーバ装置には、ドアロック制御システムが設置される家の家族構成員のそれぞれについての個人情報が収集され、その個人情報に対応して、それぞれの家族構成員が持つＩＣカードの識別情報が登録される。したがって、ドアロック制御システムは、電子鍵情報を検索することにより、それが誰の電子鍵情報であるかを判別することができる。つまり、この例の通信システムにおいては、電子鍵情報を、家族構成員の個人識別情報として用いることが可能である。

そして、管理サーバ装置に登録された各家族構成員の本鍵情報は、ド

アロック制御システムが、当該家に設置された後、システムの設置事業者や、ユーザが管理サーバ装置に対して初期登録要求をすることにより、ドアロック装置の記憶部に登録され、電子鍵情報の認証用として使用されることになる。

また、この実施形態では、本鍵装置を紛失してしまった場合を考慮して、バックアップ鍵情報を登録しておくことができる。後述するように、この実施形態では、バックアップ鍵情報は、家族構成員の各人が、バックアップ鍵装置として使用したい電子鍵装置の識別情報（この例では、ＩＣ製造番号）を管理サーバ装置に登録することにより、登録可能である。

前述したように、この実施形態においては、電子鍵情報として用いる識別情報は、個人識別情報としても用いることができることを利用して、各家族構成員個々の玄関ドアからの入退出を管理することができるようにする。

このように電子鍵情報を個人識別情報としても用いることにより、当該家に住む家族構成員それぞれの玄関ドアからの入退出の管理をすることがことができ、帰宅予定者への帰宅時刻超過の通知や、子供の帰宅の状況の親への通知などを行なえると共に、前記入退出の情報を、セキュリティシステムに反映させることができ、より高機能のセキュリティシステムを構築することができる。

[実施形態のドアロックシステムを含むセキュリティシステムの概要]

図３は、ドアロック制御システムおよびセキュリティシステムを含む、この実施形態の通信システムの概要を説明するための図である。

家の玄関ドア１には、電子鍵装置と通信を行なうドアロック装置２が取り付けられている。室内には、セキュリティシステムを構成する監視制御装置３が設けられ、ドアロック装置２と接続されている。ドアロッ

ク装置２と監視制御装置３とは、この例では接続線により接続されるが、無線により接続するようにしてもよい。

監視制御装置３は、ドアロック装置２からの電子鍵情報を受け取って、前述した電子鍵情報の認証を行なう装置、つまり認証装置となることもできる。しかし、この例では、電子鍵情報の認証は、ドアロック装置２自身において行なうようにされている。

そして、この例では、室内には、火災発生を検知する火災センサ４と、ガス漏れを検知するガスセンサ５と、窓の戸締りを検知する窓センサ６ａ，６ｂと、テレビ７が設けられ、それぞれ監視制御装置３に接続されている。監視制御装置３とそれらとの接続も、接続線により接続されているが、無線により接続してもよい。

また、図３では省略したが、火災センサ４で火災発生を検知したときに、その発生現場近傍を撮影できるような位置や、窓センサ６ａ，６ｂで賊の侵入を検知したときに、その賊を撮影できるような位置には、監視カメラを設けるようにすることができる。その場合には、それら監視カメラは監視制御装置３に接続され、監視カメラの撮影画像が監視制御装置３に供給されるようにされる。

監視制御装置３は、また、電話回線８を通じ、通信ネットワーク９を通じてセキュリティシステムの管理会社が運営する管理サーバ装置１０に接続される。この管理サーバ装置１０も、ドアロック装置２からの電子鍵情報を、監視制御装置３を介して受け取ることにより、電子鍵情報の認証を行なう装置となることもできる。

通信ネットワーク９は、携帯電話網をも含み、後述するように、監視制御装置３は、異常状態の発生時に、予め登録された携帯電話端末１１ａ，１１ｂに、当該異常状態の発生を知らせることが可能とされている。さらに、通信ネットワーク９は、インターネットを含み、パーソナルコ

ンピュータ１２は、管理サーバ装置１０に対して当該インターネットを通じてアクセスすることが可能とされている。また、携帯電話端末１１ａ，１１ｂからも、管理サーバ装置１０にアクセスすることが可能とされている。

なお、この実施形態においては、特許請求の範囲における制御装置は、ドアロック装置２の後述するドアロック制御装置と監視制御装置とで構成されるものである。

次に、ドアロック装置２の具体的構成例およびその動作、また、監視制御装置３の具体的構成例およびその動作について、詳細に説明する。なお、以下に説明する例では、前述したように、電子鍵情報の認証は、ドアロック装置自身が行なうものとする。

［電子鍵装置の構成例］

前述したように、この実施形態においては、電子鍵装置としては、ＩＣカードの他、携帯電話端末やＰＤＡ端末なども用いることができる。しかし、電子鍵装置は、生体情報の取得部と、制御用ＩＣチップと、通信手段とを備える点では共通している。電子鍵装置がＩＣカードである場合の構成例を次に示す。

＜電子鍵装置の第１の例＞

この第１の例の電子鍵装置は、生体情報として、指紋を用いるＩＣカードの場合の例である。図４Ａは、この例のＩＣカード４０Ｆの表面を示し、この表面には、所有者の氏名と、ＩＤ番号が表示されていると共に、指紋読取部４１の指紋読取窓４１Ｗが形成されている。

また、図４Ｂは、ＩＣカード４０Ｆの内部構成例を示しており、ＩＣカード４０Ｆ内には、指紋読取部４１と、後述するドアロック装置２の電子鍵リード／ライト部と通信を行なうための電磁誘導アンテナ４２と、制御用ＩＣ４３と、情報送受信回路部４４が内蔵されている。

指紋読取部４１は、指紋読取窓４１Ｗに置かれた指の指紋を読み取り、その読み取った指紋の情報を制御用ＩＣ４３に送る。制御用ＩＣ４３は、予め登録されて記憶しているＩＣカード４０Ｆの所有者の指紋情報と、読み取った指紋情報とを比較し、一致しているかどうか判別する。

そして、一致していると判別すると、予め制御用ＩＣ４３内のメモリに記憶されている電子鍵情報を読み出して、情報送受信回路部４４および電磁誘導アンテナ４２を通じて、外部に送出する。記憶している指紋情報と、読み取った指紋情報とを比較し、一致していないと判別したときには、電子鍵情報の外部への送出は禁止する。

図５は、第１の例の場合のＩＣカード４０Ｆの内部ブロック構成を示すものである。ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）４０１に対してシステムバス４０２を介してプログラムやデータが記録されているＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）４０３と、ワークエリア用ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）４０４と、電子鍵情報となる識別情報が記憶されている識別情報メモリ４０５と、通信履歴メモリ４０６と、送受信インターフェース４０７と、指紋登録メモリ４０８と、指紋読取部インターフェース４０９と、指紋照合部４１０とが接続されている。

識別情報メモリ４０５には、前述したＩＣ製造番号からなる識別情報が記憶されている。なお、このＩＣカード４０の所有者の氏名、住所の他、所有者のその他の必要な個人情報を記憶することもできる。この個人情報は、父親、母親、子供などの区別が可能なように構成される。

通信履歴メモリ４０６には、各所有者が行ったドアロック装置２の後述する電子鍵リード／ライト部との通信の時刻や履歴（内側と外側のどちらの電子鍵リード／ライト部と通信したか情報を含む）や、各所有者の外出、帰宅の履歴などを書き込むことが可能とされている。なお、こ

れらの履歴情報は、後述するように、ドアロック装置２のメモリや監視制御装置３のメモリにおける家族構成員の各人に対応するエリアにも記憶されるものである。

送受信インターフェース４０７には、電磁誘導アンテナ４１に接続されている情報送受信回路部４４が接続されている。

指紋登録メモリ４０８には、当該ＩＣカード４０Ｆの所有者の指紋の情報が予め登録されて記憶されている。指紋読取部インターフェース４０９は、指紋読取部４１で読み取った指紋の情報を取り込むためのものである。指紋照合部４１０は、指紋読取部インターフェース４０９を通じて取得した指紋の情報と、指紋登録メモリ４０８から読み出した前記所有者の指紋の情報とを比較し、一致しているか否かを判定して、その判定結果をシステムバス４０２に送出する。指紋照合部４１０は、ハードウエアの構成ではなく、ＣＰＵ４０１によるソフトウエアによる構成とすることもできる。

ＣＰＵ４０１は、前述したように、指紋照合部４１０での判定結果に基づき、指紋一致、つまり、指紋照合がＯＫであったときには、識別情報メモリ４０５から読み出した識別情報からなる電子鍵情報を、送受信インターフェース４０７、情報送受信回路４０８および電磁誘導アンテナ４１を通じて送出し、指紋照合部４１０での判定結果が指紋不一致、つまり、指紋照合がＮＧであったときには、電子鍵情報の送出を禁止する。

また、ＣＰＵ４０１は、電磁誘導アンテナ４２にて受信した情報を、情報送受信回路部４４および送受信インターフェース４０７を通じて取り込み、通信履歴メモリ４０６に書き込んだりする処理も行なう。

図６は、このときのＣＰＵ４０１での処理動作を説明するためのフローチャートである。

ＣＰＵ４０１は、指紋読取部インターフェース４０９を通じた指紋読取部４１からの指紋情報の受信を待ち（ステップＳ１）、指紋情報を受信したと判別したときには、指紋登録メモリ４０８に登録されている所有者の指紋情報を読み出し、指紋照合部４１０において指紋照合を行なわせる（ステップＳ２）。

そして、ＣＰＵ４０１は、指紋照合部４１０からの指紋照合の判定結果が指紋一致であるか否か判別し（ステップＳ３）、指紋不一致で照合がＮＧであったときには、処理をそのまま終了して、電子鍵情報の送出は行なわない。

また、ＣＰＵ４０１は、指紋一致で照合がＯＫであったときには、識別情報メモリ４０５から識別情報を読み出して、電子鍵情報として、情報送受信回路部４４および電磁誘導アンテナ４２を通じて送出する（ステップＳ４）。

そして、ＣＰＵ４０１は、相手方のリード／ライト部と通信を行なったか否か判別し（ステップＳ５）、電磁誘導アンテナ４２、情報送受信回路部４４および送受信インターフェース４０７を通じて相手方から所定の情報を受け取ったときには、相手方との通信を行なったとして、通信履歴を通信履歴メモリ４０６に書き込み（ステップＳ６）、その後、この処理ルーチンを終了する。

ステップＳ５で、相手方のリード／ライト部からの情報を受信せず、通信を行っていないと判別したときには、ＣＰＵ４０１は、電子鍵情報を送出してから予め定めた所定時間、経過したか否か判別し（ステップＳ７）、所定時間経過していないと判別したときには、ステップＳ４に戻り、電子鍵情報を再度送って相手方からの情報を待つ。そして、ステップＳ７で、所定時間経過したと判別したときには、この処理ルーチンをそのまま終了する。

以上のように、この例の電子鍵装置としてのＩＣカード４０Ｆによれば、予め登録してある所有者の指紋と、使用者の指紋とを照合して、照合がＯＫである場合にのみ電子鍵情報の送出を行なうので、予め登録された使用者しか、当該電子鍵装置を使用できず、もしも、当該電子鍵装置を紛失したとしても、他の使用者の使用を阻止することができる。

＜電子鍵装置の第２の例＞

この第２の例の電子鍵装置は、生体情報として、虹彩を用いるＩＣカードの場合の例である。図７Ａは、この例のＩＣカード４０Ｉの表面を示し、この表面には、所有者の氏名と、ＩＤ番号が表示されていると共に、使用者の虹彩を読み取るための手段として、この例では、ＣＣＤ（Ｃｈａｒｇｅ　Ｃｏｕｐｌｅｄ　Ｄｅｖｉｃｅ）カメラ４５が設けられている。

また、図７Ｂは、ＩＣカード４０Ｉの内部構成例を示しており、ＩＣカード４０Ｉ内には、第１の例のＩＣカード４０Ｆと同様に、電磁誘導アンテナ４２と、制御用ＩＣ４３と、情報送受信回路部４４とが内蔵されていると共に、ＣＣＤカメラ４５からの撮像信号を処理して制御用ＩＣ４３に供給するための撮像信号処理回路部４６が内蔵されている。

使用者は、ＣＣＤカメラ４５により自分の目（虹彩）を撮影させる。ＣＣＤカメラ４５は、撮影した使用者の虹彩情報を撮像信号処理回路部４６を通じて取り込み、その取り込んだ虹彩の情報を制御用ＩＣ４３に送る。制御用ＩＣ４３は、予め登録されて記憶されているＩＣカード４０Ｉの所有者の虹彩情報と、取り込んだ虹彩情報とを比較し、一致しているかどうか判別する。

そして、一致していると判別すると、予め制御用ＩＣ４３内のメモリに記憶されている電子鍵情報を読み出して、情報送受信回路部４４および電磁誘導アンテナ４２を通じて、外部に送出する。記憶している虹彩

情報と、取り込んだ虹彩情報とを比較し、一致していないと判別したときには、電子鍵情報の外部への送出は禁止する。

図８は、第２の例の場合のＩＣカード４０Ｉの内部ブロック構成を示すものである。この第２の例においては、図５の第１の例の指紋登録メモリ４０８と、指紋読取部インターフェース４０９と、指紋照合部４１０とに代わって、虹彩情報登録メモリ４１１と、撮像信号インターフェース４１２と、虹彩照合部４１３とが設けられる。撮像信号インターフェース４１２は、ＣＣＤカメラ４５に接続されている。その他の構成は、第１の例の図５と同様である。

虹彩情報登録メモリ４１１には、当該ＩＣカード４０Ｉの所有者の虹彩の情報が予め登録されて記憶されている。撮像信号インターフェース４１２は、撮像信号処理回路部４６からの虹彩情報を取り込むためのものである。虹彩照合部４１３は、撮像信号インターフェース４１２を通じて取り込んだ虹彩情報と、虹彩情報登録メモリ４１１から読み出した前記所有者の虹彩情報とを比較し、一致しているか否かを判定して、その判定結果をシステムバス４０２に送出する。虹彩照合部４１３は、ハードウエアの構成ではなく、ＣＰＵ４０１によるソフトウエアによる構成とすることもできる。

ＣＰＵ４０１は、虹彩照合部４１３での判定結果に基づき、虹彩一致、つまり、虹彩照合がＯＫであったときには、識別情報メモリ４０５から読み出した識別情報からなる電子鍵情報を、送受信インターフェース４０７、情報送受信回路４４および電磁誘導アンテナ４１を通じて送出し、虹彩照合部４１３での判定結果が虹彩不一致、つまり、虹彩照合がＮＧであったときには、電子鍵情報の送出を禁止する。

図９は、このときのＣＰＵ４０１での処理動作を説明するためのフローチャートである。

ＣＰＵ４０１は、撮像信号インターフェース４１２を通じた撮像信号処理回路部４６からの虹彩情報の受信を待ち（ステップＳ１１）、虹彩情報を受信したと判別したときには、虹彩情報登録メモリ４１１に登録されている所有者の虹彩情報を読み出し、虹彩照合部４１３において虹彩照合を行なわせる（ステップＳ１２）。

そして、ＣＰＵ４０１は、虹彩照合部４１３からの虹彩照合の判定結果が虹彩一致であるか否か判別し（ステップＳ１３）、虹彩不一致で照合がＮＧであったときには、処理をそのまま終了して、電子鍵情報の送出は行なわない。

また、ＣＰＵ４０１は、虹彩一致で照合がＯＫであったときには、識別情報メモリ４０５から識別情報を読み出して、電子鍵情報として、情報送受信回路部４４および電磁誘導アンテナ４２を通じて送出する（ステップＳ１４）。

そして、ＣＰＵ４０１は、相手方のリード／ライト部と通信を行なったか否か判別し（ステップＳ１５）、電磁誘導アンテナ４２、情報送受信回路部４４および送受信インターフェース４０７を通じて相手方から所定の情報を受け取ったときには、相手方との通信を行なったとして、通信履歴を通信履歴メモリ４０６に書き込み（ステップＳ１６）、その後、この処理ルーチンを終了する。

ステップＳ１５で、相手方のリード／ライト部からの情報を受信せず、通信を行っていないと判別したときには、ＣＰＵ４０１は、電子鍵情報を送出してから予め定めた所定時間、経過したか否か判別し（ステップＳ１７）、所定時間経過していないと判別したときには、ステップＳ１４に戻り、電子鍵情報を再度送って相手方からの情報を待つ。そして、ステップＳ７で、所定時間経過したと判別したときには、この処理ルーチンをそのまま終了する。

以上のように、この第２の例の電子鍵装置としてのＩＣカード４０Ｉによれば、予め登録してある所有者の虹彩と、使用者の虹彩とを照合して、照合がＯＫである場合にのみ電子鍵情報の送出を行なうので、予め登録された使用者しか、当該電子鍵装置を使用できず、もしも、当該電子鍵装置を紛失したとしても、他の使用者の使用を阻止することができる。

［生体情報の他の例］

以上の例では、生体情報としては、指紋と、虹彩の場合について説明したが、生体情報としては、これに限られるものではない。例えば手の甲の静脈パターンを生体情報として用いることもできる。この場合には、虹彩情報に代えて、所有者の手の甲の静脈パターンを登録して記憶しておくとともに、ＣＣＤカメラ４５により、手の甲の静脈パターンを撮影して取り込むことにより、第２の例のＩＣカード４０Ｉの構成をそのまま用いることができる。

なお、以上の例に限らず、個人識別が可能な生体情報であって、所定の手段により取得可能なものであれば、どのような生体情報も、利用することができることは勿論である。

［ドアロック装置の構成］

図１０Ａおよび図１０Ｂは、ドアロック装置２の構成例を説明するための図である。図１０Ａは、家の外側から玄関ドア１のドアロック装置２の取り付け部分近傍を見た図である。また、図１０Ｂは、玄関ドア１のドアロック装置２の取り付け部分近傍を、玄関ドア１の端面側から見た図である。

この例のドアロック装置２においては、玄関ドア１の外側（戸外側）には、電子鍵装置の例としてのＩＣカード４０Ｆや４０Ｉと通信を行なうための外側電子鍵リーダ／ライタ部２１ｅｘと、電子鍵情報の認証結

果や玄関ドア１の施錠または開錠を視覚的に知らせるための表示素子の例としての外側ＬＥＤ（Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ；発光ダイオード）２２ｅｘと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を音声により知らせるための外側スピーカ２３ｅｘと、外側ドアノブ２４ｅｘとが設けられている。

また、玄関ドア１の内側（屋内側）にも、電子鍵装置の例としてのＩＣカード４０Ｆや４０Ｉと通信を行なうための内側電子鍵リーダ／ライタ部２１ｉｎと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を視覚的に知らせるための表示素子の例としての内側ＬＥＤ２２ｉｎと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を音声により知らせるための内側スピーカ２３ｉｎと、内側ドアノブ２４ｉｎとが設けられている。

玄関ドア１には、さらに、玄関ドア係止片２５と、ロック片２６と、ドア開閉センサ２７が設けられている。さらに、玄関ドア１の内側には、ドアロック装置２の動作を制御するためのドアロック制御装置１００が設けられており、電子鍵リーダ／ライタ部２１ｅｘおよび２１ｉｎ、ＬＥＤ２２ｅｘおよび２２ｉｎ、スピーカ２３ｅｘおよび２３ｉｎ、ドア開閉センサ２７および図示を省略したドアロック機構駆動部が、このドアロック制御装置１００に接続されている。

玄関ドア係止片２５は、ドアノブ２４ｅｘあるいはドアノブ２４ｉｎの操作に応じて、玄関ドアの端面１ａに垂直な方向に摺動移動する部材である。これは、後述するオートロックモードでない場合において、玄関ドア１が施錠されていないときにも、玄関ドア１の端面１ａと対向する壁の端面側に設けられる凹部に勘合して、玄関ドア１を、係止するためのものである。

ロック片２６は、ドアロック機構の一部を構成する部材であり、図１

０Ａおよび図１０Ｂでは図示を省略したドアロック機構駆動部によりドアロック機構が駆動されることにより、玄関ドアの端面１ａに垂直な方向に摺動移動して、玄関ドア１を施錠するときには、図１０Ａのように、玄関ドア１の端面１ａから突出する状態に固定され、玄関ドア１を開錠するときには、玄関ドア１の端面１ａから突出しない状態に固定される。

なお、図示は省略したが、玄関ドア１の端面１ａと対向する壁の端面には、このロック片２６が突出した状態のときに嵌合される凹部が形成されており、ロック片２６が当該凹部に嵌合される状態が玄関ドアの施錠状態となる。そして、ロック片２６が玄関ドア１側に引っ込んで、当該凹部に嵌合していないときには、施錠状態が解除されて、開錠状態になる。

玄関ドア開閉センサ２７は、例えば光学式センサが用いられ、玄関ドア１が開けられたときは外部光を検知することにより、それを検知し、玄関ドア１が閉じられたときには、玄関ドア１の端面１ａが、壁の端面と衝合することにより外部光が遮断されることを検知することにより、それを検知して、玄関ドア１の開閉を検知する。

［ドアロック制御装置１００の説明］

次に、ドアロック制御装置１００を中心にしたドアロック装置２の電気的な構成例を図１１に示す。なお、以下の説明においては、電子鍵装置としては、指紋照合認証を行なう第１の例のＩＣカード４０Ｆを用いるものとする。

すなわち、ドアロック制御装置１００は、マイクロコンピュータの構成を備えており、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１０１に対してシステムバス１０２を介してプログラムやデータが記録されているＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１０３と、ワークエリア用ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏ

ｒｙ）１０４と、家族構成員の個々についての電子鍵情報となる識別情報（この例では、ＩＣ製造番号）が記憶されている家族情報メモリ１２０と、監視制御装置３と通信を行なうための通信インターフェース１２１と、時計回路１２２が接続されている。

家族情報メモリ１２０には、後述するように、管理サーバ装置１０に登録された本鍵情報やバックアップ鍵情報が、家族構成員のそれぞれについて、電子鍵情報として登録されて格納されている。また、各家族構成員を識別するための情報、例えば、氏名、年齢、性別、続き柄、その他の個人情報も、併せて家族情報メモリ１２０に格納するようにしてもよい。この家族情報メモリ１２０への電子鍵情報の登録に関しては、後述する。

また、システムバス１０２には、インターフェース１０５および１０６を介して内側電子鍵リード／ライト部２１ｉｎおよび外側電子鍵リード／ライト部２１ｅｘが接続され、また、内側ＬＥＤ駆動部１０７を介して内側ＬＥＤ２２ｉｎが接続され、外側ＬＥＤ駆動部１０８を介して外側ＬＥＤ２２ｅｘが接続され、さらに、音声出力インターフェース１０９を介して内側スピーカ２３ｉｎが接続され、音声インターフェース１１０を介して外側スピーカ２３ｅｘが接続される。

さらに、システムバス１０２には、インターフェース１１１を介してドア開閉センサ２７が接続されると共に、ドアロック機構駆動部１１２を介して、ロック片２６を摺動駆動させるドアロック機構２８が接続される。

電子鍵リード／ライト部２１ｅｘまたは２１ｉｎは、ＩＣカード４０Ｆ（または４０Ｉ）と通信を行なう通信部を構成する。電子鍵リード／ライト部２１ｅｘまたは２１ｉｎは、この例では、電磁誘導アンテナおよび情報送受信部を含む。

この例のドアロック制御装置１００は、ドアロック制御モードとして、オートロックモードと、逐次ロックモードとの２通りの制御モードを備えている。

オートロックモードは、ドアロック制御装置１００が、電子鍵リード／ライト部２１ｅｘ，２１ｉｎを介してＩＣカード４０Ｆと通信することに基づき玄関ドア１を開錠した後、所定時間後に自動的に玄関ドアを施錠状態にするモードである。オートロックモードにおいては、常に、内側と外側の電子鍵リード／ライト部２１ｅｘ，２１ｉｎの両方を用いるものとなる。

また、逐次ロックモードは、少なくとも玄関ドア１の外側の電子鍵リード／ライト部２１ｅｘを通じてＩＣカード４０Ｆと通信することに基づき玄関ドアの施錠、開錠の状態を、そのときの状態とは逆の状態にするモードである。この逐次ロックモードにおいても、内側と外側の電子鍵リード／ライト部２１ｅｘ，２１ｉｎの両方を用いることができるが、内側は、別途のマニュアルの施錠手段により施錠するようにした場合には、外側の電子鍵リード／ライト部２１ｅｘを通じたＩＣカード４０Ｆとの通信のみにより、玄関ドアの施錠、開錠動作を行なわせるようにすることができる。この逐次ロックモードは、従来からの一般的な鍵による施錠、開錠の方法に合わせたモードである。

ドアロック装置２のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、この例では、例えば、ドアロック装置２を取り付ける際に、後述するように、作業者により監視制御装置３を通じて行なわれる。

ドアロック装置２がいずれのドアロック制御モードに設定されているかの情報は、ドアロック制御装置１００内の図示を省略した不揮発性メモリに格納されており、ドアロック制御装置１００は、当該不揮発性メ

モリの記憶情報を参照することにより、自装置のドアロック制御モードが、オートロックモードか、逐次ロックモードかを認識するものである。監視制御装置３を通じたドアロック制御モードの設定動作に関しては、後述する。

なお、ドアロック装置２のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、監視制御装置３を通じて行なうのではなく、ドアロック装置２に直接的に行なうようにすることもできる。例えば、予め、ドアロック装置２の出荷時に、いずれのドアロック制御モードにするかの設定をドアロック装置２に行なっておくようにしても良い。また、ドアロック装置２に、ドアロック装置２の設置作業者が操作可能な入力操作手段、例えばディップスイッチ等を設けておき、当該入力操作手段を通じて、ドアロック制御モードの設定を行なうようにしてもよい。

［監視制御装置３の外観の説明］

図１２は、室内に設けられるセキュリティシステム用の監視制御装置３の構成を説明するための外観図であり、この監視制御装置３は、例えば赤外線や電波を用いたリモートコマンダ５０によりリモコン制御可能の構成とされている。

監視制御装置３の筐体３０には、ビデオカメラ３１が組み込まれている。このビデオカメラ３１は、この例では、実線位置の横置き状態と、点線位置の縦置き状態とのいずれの状態をも取れる機構により、筐体３０に対して取り付けられている。このビデオカメラ３１は、セキュリティモードがオンとされたときに、監視制御装置３からの指示により撮影を開始するようにされている。

また、ビデオカメラ３１による撮影方向は、ビデオカメラが首振り方向に調整可能な構造とされているので、その調整により変えられるよう

にされている。したがって、使用者は、セキュリティモードオンに先立ち、ビデオカメラ３１による撮影方向の調整を行なっておくことができる。

そして、筐体３０には、ビデオカメラ３１による撮影対象部を明るく照明するための撮影用ランプ３２が設けられている。また、筐体３０には、例えば遠赤外線を検知することにより人を検知する人感センサ３３が設けられている。監視制御装置３は、後述するように、セキュリティモードオンのときに人感センサ３３で人を検知したときには、賊の侵入であるとして検知し、撮影用ランプ３２をオンにすると共に、所定の通報先に撮影画像を送るようにする。

筐体３０には、また、マイクロホン３４とスピーカ３５とが設けられている。マイクロホン３４は、賊の声や賊侵入時の室内の臨場音を収音するためのものである。スピーカ３５は、侵入してきた賊を威嚇する音声を放音するためなどに用いられる。

筐体３０には、また、電子鍵リード／ライト部３６が設けられる。この電子鍵リード／ライト部３６は、この例では、伝言の記録、再生の際に用いられる。すなわち、この例においては、監視制御装置３は、伝言装置の役割もできるように構成されており、電子鍵リード／ライト部３６により、電子鍵装置としてのＩＣカード４０Ｆを読み取らせた後、後述するようにリモートコマンダ５０の伝言記録ボタンを押すと、設定した相手（家族の誰か）に伝言が残すことができ、また、リモートコマンダ５０の伝言再生ボタンを押すと、自分宛ての伝言を再生することができるようになっている。

この伝言が記録されているかどうかなどを知らせるため等の用途として、筐体３０には、複数個のＬＥＤ３７が設けられている。また、筐体３０には、さらに、リモートコマンダ５０からのリモコン信号の受信部

３８が設けられる。

また、図１２では図示を省略したが、監視制御装置３の背面パネルには、テレビ受像機７のビデオ入力端子に接続される映像出力端子が設けられている。そして、監視制御装置３には、テレビ受像機７の電源のオン・オフなどを制御するためのリモコン送信部３９が設けられている。

さらに、監視制御装置３は、火災センサ４、ガスセンサ５、窓センサ６ａ，６ｂ、さらには、監視カメラを接続するためのセンサハブを備えている。また、図３で説明したように、監視制御装置３は、電話回線を通じて、セキュリティシステムの管理会社が運営する管理サーバ装置１０にアクセスできるように構成されている。

［監視制御装置３の構成例］

監視制御装置３の内部構成および監視制御装置３と周辺機器との接続状態の構成例を図１３に示す。

監視制御装置３は、マイクロコンピュータの構成を備えており、ＣＰＵ２０１に対して、システムバス２０２を介して、プログラムやデータが記録されているＲＯＭ２０３と、ワークエリア用ＲＡＭ２０４と、ドアロック制御装置１００の家族情報メモリ１２０と同様に、電子鍵装置としてのＩＣカード４０Ｆまたは４０Ｉを所有する家族全員の電子鍵情報となる識別情報が記憶されている家族情報メモリ２０５と、ドアロック制御装置１００と通信を行なうためのドアロック装置通信インターフェース２０６と、センサハブ２０７と、ビデオカメラ３１の撮影画像およびマイクロホン３４で収音した音声を記憶するための画像・音声メモリ２０８と、電話回線を通じて管理サーバ装置１０等と通信を行なうための通信インターフェース２０９とが接続されている。

また、システムバス２０２には、カメラインターフェース２１０を介してビデオカメラ３１が、インターフェース２１１を介して撮影用ラン

プ３２の照明機構３２０が、インターフェース２１２を介して人感センサ３３が、インターフェース２１４を介して電子鍵リード／ライト部３６が、インターフェース２１５を介してリモコン受信部３８が、インターフェース２１６を介してリモコン送信部３９が、音声入力インターフェース２１８を介してマイクロホン３４が、インターフェース２１９を介してＬＥＤ３７が、音声出力インターフェース２２０を介してスピーカ３５が、それぞれ接続されている。

さらに、システムバス２０２は、ビデオ信号出力端子からなるテレビインターフェース２１７を介してテレビ受像機７に接続されている。また、システムバス２０２には、時計回路２２１と、通知連絡設定メモリ２２２とが接続されている。

家族情報メモリ２０５は、例えばＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）で構成される。

家族情報メモリ２０５には、ドアロック制御装置１００の家族情報メモリ１２０と同様に、家族構成員のそれぞれについての識別情報と、個人情報とが格納されている。この明細書では、識別情報と個人情報とからなる情報を、個人プロファイル情報と呼ぶことにする。

後述するように、この例では、家族構成員すべての個人プロファイル情報は、ドアロック装置２および監視制御装置３が設置されたときに、設置管理者が管理サーバ装置１０に初期登録依頼をすることにより、管理サーバ装置１０から送られてきて、監視制御装置３に自動的に登録される。そして、監視制御装置３は、少なくとも個人プロファイル情報のうちの個人識別情報を電子鍵情報として、ドアロック制御装置１００に転送する。ドアロック制御装置１００は、その電子鍵情報を家族情報メモリ１２０に登録する。

図１４に、一人分の個人プロファイル情報の例を示す。図１４に示すように、個人プロファイル情報は、個人識別情報と個人情報とが対応付けられて記憶された情報である。この実施形態では、個人識別情報は、前述したように、電子鍵装置の各メモリに格納されている識別情報が用いられる。個人識別情報は個人情報と対応させることで、具体的に誰の識別情報であるかが判明する。この識別情報は、電子鍵情報の役割を有することは前述した通りであり、図１４に示すように、電子鍵情報としては、本鍵情報とバックアップ鍵情報とが登録可能である。バックアップ鍵情報は、複数個、登録可能としてもよい。

図１４の例においては、個人情報としては、個人識別情報以外の情報であり、パスワード情報、氏名、住所、生年月日、年齢、続柄、登録日、銀行口座番号、電話番号、電子メールアドレス、ＩＰアドレス、趣味／嗜好情報、家の玄関８からの入退出履歴情報、電子鍵登録・紛失履歴情報などが家族情報メモリ２０５に記憶される。

この例の入退出履歴情報には、外出時刻、帰宅時刻が記憶されるほか、外出中であるか、在宅であるかの在／不在フラグが含まれる。この入退出履歴情報は、監視制御装置３が玄関ドア７を通じての家族の入退出を管理するために用いられる。また、電子鍵登録・紛失履歴情報は、後述するように、管理サーバ装置１０からの電子鍵情報のバックアップ登録要求や抹消要求が到来して、バックアップ登録や抹消処理をしたときに、その日付、時刻とともに、バックアップ鍵情報や抹消した電子鍵情報を、バックアップ登録および抹消の区別をして記録しておくものである。

さらに、この例では、この家族情報メモリ２０５には、セキュリティモード用の情報も格納されている。すなわち、この例では、監視制御装置３では、家族構成員の在宅状況に応じて、セキュリティレベルを変更することが可能なように構成されている。図１５は、セキュリティレベ

ルと家族構成員の在宅状況との関係を示すテーブルである。また、図１６は、セキュリティレベルとセキュリティ内容との対応を示すテーブルである。

図１６に示すように、この例においては、セキュリティレベルは、セキュリティレベルが高い方から順に、レベルＡ、レベルＢ、レベルＣ、レベルＤまであり、レベルＡにおいては、窓および玄関ドアの監視、火災やガス漏れの監視、ビデオカメラ３１による監視の全てを行ない、レベルＢでは、ビデオカメラ３１による監視は行なわずに、窓および玄関ドアの監視および火災やガス漏れの監視を行ない、レベルＣでは、火災やガス漏れの監視のみを行ない、レベルＤでは、監視を行なわない、という内容である。

そして、図１５に示すように、家族構成員の在宅状況のそれぞれに対して各セキュリティレベルが割り付けられる。すなわち、この例では、父親が在宅の状況では、監視を行なわないレベルＤとされる。また、父親が不在であるが母親が在宅の状況では、火災やガス漏れの監視のみを行なうレベルＣとされる。また、子供のみが在宅の状況では、窓および玄関ドアの監視および火災やガス漏れの監視を行なうレベルＢとされる。そして、全員が不在である状況では、全ての監視を行なうレベルＡとされる。

監視制御装置３では、セキュリティモードをオンにするとき、また、セキュリティレベルを変更するとき、これら図１５、図１６のテーブルを参照し、在宅状況に応じてセキュリティレベルを決定するようにする。

図１５のセキュリティレベルと、家族構成員の在宅状況との関係は、予め設定しておくこともできるし、使用者が、例えばリモートコマンダ５０を用いて監視制御装置３に入力設定することにより、設定を変更することできるように構成されている。

なお、これら図１５、図１６のテーブル情報は、家族情報メモリ２０５ではなく、別のメモリに格納するようにしても良いことは言うまでもない。

ドアロック装置通信インターフェース２０６は、ドアロック制御装置１００に接続されている。センサハブ２０７には、火災センサ４、ガスセンサ５、窓センサ６ａ，６ｂおよび１個あるいは複数個の監視カメラ１３が接続される。

画像・音声メモリ２０８は、セキュリティモードがオンであるときに、ビデオカメラ３１で撮影した画像情報と、マイクロホン３４で収音した音声情報とをバッファリングする監視情報領域と、伝言として記録されている画像情報および音声情報を記憶する伝言情報領域とを備えている。また、監視情報領域には、監視カメラ１３用の画像記憶領域も設けられている。

監視情報領域は、この例では、所定時間、例えば３０秒分の画像情報および音声情報を、いわゆるリングバッファ形式で記憶する。なお、監視情報領域と伝言情報領域とは、別々のメモリの構成とすることも勿論できる。

通信インターフェース２０９は、この例では、ルータ６１に接続されている。ルータ６１は、ＡＤＳＬモデム６２、スプリッタ６３を通じて電話回線６５に接続されている。スプリッタ６３には、電話端末６４が接続される。

時計回路２２１は、現在時刻の情報をシステムバス２０２に送出する。現在時刻の情報には、年、月、日、曜日などのいわゆるカレンダー情報も含む。

通知連絡設定メモリ２２２は、後述するように、使用者により、リモートコマンダ５０が用いられて設定された帰宅予定者、外出予定者、帰

宅予定時刻、外出予定時刻、通知連絡者などの設定情報を記憶する。ＣＰＵ２０１は、この設定情報に基づいて、設定された通知連絡者に、帰宅予定者や外出予定者の帰宅状況や帰宅時刻、外出状況や外出時刻などを通知連絡するようにする。設定動作や通知連絡の動作に関しては、後述する。

［リモートコマンダ５０の説明］

監視制御装置３用のリモートコマンダ５０は、図１２に示すように、セキュリティボタン５１と、オフボタン５２と、伝言記録ボタン５３と、伝言再生ボタン５４と、メニューボタン５５と、上下左右の選択を行なう４個のキーとその中央の決定キーとからなるカーソルボタン５６とを備えて構成されている。

メニュー項目としては、この例では、管理サーバ装置１０に対する電子鍵情報としての個人ＩＤの登録、ドアロック装置２のドアロック制御モードの設定、その他が、用意されており、それぞれのメニュー項目に対応する処理を実行するアプリケーションプログラムは、監視制御装置３のＲＯＭ２０３に格納されている。

［管理サーバ装置１０の構成］

次に、管理サーバ装置１０の構成例を図１７に示す。管理サーバ装置１０は、コンピュータの構成を備えており、ＣＰＵ３０１に対して、システムバス３０２を介して、プログラムやデータが記録されているＲＯＭ３０３と、ワークエリア用ＲＡＭ３０４と、ドアロック装置管理データベース３０５と、電子鍵登録・紛失履歴メモリ３０６と、インターネットなどの通信ネットワークを通じて通信を行なうための通信インターフェース３０７とが接続されている。また、システムバス３０２には、さらに、ホームページ用メモリ３０８と、画像・音声メモリ３０９とが接続されている。

ドアロック装置管理データベース３０５には、ドアロック装置２および監視制御装置３のシリアル番号、ドアロック装置２および監視制御装置３が設置された住所、電話番号、ＩＰアドレス、ドアロック装置の利用者の氏名、登録された電子鍵情報を個人プロファイル情報など、ドアロック装置２の管理に必要な事項が格納されている。電話番号、ＩＰアドレスは、ドアロック装置２および監視制御装置３の通信ネットワーク９上のアドレス情報である。

電子鍵登録・紛失履歴メモリ３０６には、各ドアロック装置２ごとに、電子鍵情報の登録と紛失の履歴が記憶される。ホームページ用メモリ３０８には、ホームページの各ページの表示情報が格納されており、ＣＰＵ３０１の指示に従い、必要なページの表示情報が、このメモリ３０８から読み出されて、通信インターフェース３０７を通じて通信ネットワークに送出される。

画像・音声メモリ３０９は、後述するように、セキュリティ監視システムから送られてくる画像・音声情報を格納する。管理サーバ装置１０では、セキュリティ監視システムからの画像・音声をチェックして、警備会社に通知したり、ユーザの求めに応じて、画像・音声情報をホームページを通じて提供するようにする。

次に、以上のような構成の通信システムにおける種々の動作について、以下に説明する。

［監視制御装置３における伝言記録および伝言再生；図１８］

前述したように、この例の監視制御装置３は、電子鍵装置、この例ではＩＣカード４０Ｆと、リモートコマンダ５０を用いて、特定の家人を指定して、伝言を記録しておくことができる。伝言が監視制御装置３に記録されているときには、ＬＥＤ３７が点灯あるいは点滅して、その旨を知らせるようにしている。

そして、監視制御装置３に、伝言が記録されている場合には、帰宅した家人が、自分の電子鍵装置としてのＩＣカード４０Ｆを、この電子鍵リード／ライト部３６により読み取らせ、リモートコマンダ５０により伝言再生を指示すると、記録されている伝言が、その人宛ての伝言である場合には、監視制御装置３は、記録されている伝言を、テレビ受像機７やスピーカ３５を通じて再生するようにするように構成されている。

図１８は、この伝言記録および再生のための監視制御装置３の処理を説明するためのフローチャートである。この図１８の各ステップＳの処理は、ＣＰＵ２０１がＲＯＭ２０３に記憶されているプログラムにしたがって実行されるものである。

すなわち、まず、使用者は、伝言記録または伝言再生をするには、自分のＩＣカード４０Ｆを電子鍵リード／ライト部３６にかざして、通信を行なうようにする。ＣＰＵ２０１は、電子鍵リード／ライト部３６でＩＣカード４０Ｆと通信が行なわれたか否か判別し(ステップＳ２１)、通信が行われたと判別すると、受信した識別情報により、誰のＩＣカード４０Ｆと通信したかを認識する（ステップＳ２２）。

次に、リモートコマンダ５０からのリモコン信号の到来を待ち（ステップＳ２３）、リモコン信号を受信したことを確認したら、そのリモコン信号は、伝言記録ボタン５３の操作によるものか否か判別し（ステップＳ２４）、伝言記録ボタン５３の操作によるものであると判別したときには、ＣＰＵ２０１は、伝言記録動作を行なうようにする（ステップＳ３３）。

この伝言記録動作においては、監視制御装置３は、ビデオカメラ３１で撮影された伝言者の画像情報をカメラインターフェース２１０を介して取り込み、画像・音声メモリ２０８の伝言記録領域に格納すると共に、マイクロホン３４で収音した伝言音声情報（伝言メッセージ）をインタ

ーフェース２１８を通じて取り込み、画像・音声メモリ２０８の伝言記録領域に格納する。このとき、それら画像情報および音声情報は、電子鍵装置４０から読み込んだ識別情報に対応付けられて、当該識別情報と共に画像・音声メモリ２０８に格納される。

次に、ＣＰＵ２０１は、家族情報メモリ２０８に記憶されている家族の個人プロファイル情報を参照して、伝言記録をしようとしている操作者以外の伝言相手のリストをテレビ受像機７の画面に表示する（ステップＳ３４）。このとき、テレビ受像機７に電源が投入されていないときには、リモコン送信部３８を通じて電源をオンにするリモコン信号をテレビ受像機７に供給して、テレビ受像機７に電源を投入しておく。なお、伝言相手のリストの画面は、例えばスーパーインポーズによりテレビ番組の画像に重ねて表示するようにしてもよいし、テレビ番組の画像に重ねることなく単独の画面としてもよい。

操作者は、この伝言相手のリストから、リモートコマンダ５０のカーソルキー５６を用いて、伝言相手の選択入力を行ない、カーソルキー５６中の中央の決定キーを押す。監視制御装置３のＣＰＵ２０１は、この伝言相手の選択入力を受信して（ステップＳ３５）、当該伝言相手の情報を、画像・音声メモリ２０８の伝言記録領域の、前記画像情報および伝言音声メッセージに対応させて格納して登録する（ステップＳ３６）。そして、伝言が記録されたことを報知するために、１個のＬＥＤ３７を点灯させる（ステップＳ３７）。ＬＥＤ３７は、図１２に示したように複数個設けられており、記録されている伝言の数だけ、点灯することとなる。

また、ステップＳ２４において、リモコン信号が伝言記録ボタン５３の操作によるものではないと判別したときには、伝言再生ボタン５４の操作によるものであるか否か判別する（ステップＳ２５）。伝言再生ボ

タン５４の操作によるものでないと判別したときには、ＣＰＵ２０１は、当該操作されたボタンに応じた処理を行なう（ステップＳ２６）。

そして、ステップＳ２５において、伝言再生ボタン５４の操作によるものであると判別したときには、ＣＰＵ２１は、ステップＳ２２で認識した識別情報を検索子として、画像・音声メモリ２０８の伝言記録領域の記憶内容を検索して、ＩＣカード４０Ｆを電子鍵リード／ライト部３６にかざした操作者宛ての伝言があるか否か判別する（ステップＳ２７）。

そして、ステップＳ２７において、操作者宛ての伝言が無いと判別したときには、ＣＰＵ２０１は、例えば予めＲＯＭ２０３に用意されている「伝言はありません」の文字情報をテレビ受像機７の画面に表示すると共に、スピーカ３５を通じて音声として放音して、操作者に報知する（ステップＳ２８）。

また、ステップＳ２７において、操作者宛ての伝言が有ると判別したときには、当該操作者宛ての伝言画像および伝言音声を画像・音声メモリ２０８から読み出して、テレビ受像機７に表示すると共に、スピーカ３５から放音して再生する（ステップＳ２９）。

伝言の再生が終了すると、ＣＰＵ２０１は、テレビ受像機７の画面に伝言を消去するかどうかの問い合わせを表示するので、操作者は、その表示画面に含まれる「ＹＥＳ」、「ＮＯ」のいずれかをリモートコマンダ５０のカーソルキー５６を用いて選択する。ＣＰＵ２０１は、当該操作者の選択入力から、伝言を消去するか否か判別し（ステップＳ３０）、消去すると判別したときには、画像・音声メモリ２０８の対応する画像・音声情報を消去し（ステップＳ３１）、点灯しているＬＥＤ３７の一つを消灯する（ステップＳ３２）。そして、この伝言記録再生処理ルーチンを終了する。

また、ステップＳ３０で、伝言を消去しないと判別したときには、そ

のまま、この伝言記録再生処理ルーチンを終了する。

［ドアロック制御モードの選択設定；図１９、図２０］

前述したように、この実施形態では、監視制御装置３を通じてドアロック制御モードの設定ができるようにされているので、その設定動作を、図１９のフローチャートを参照しながら説明する。

先ず、監視制御装置３のＣＰＵ２０１は、リモコン受信部３８の受信信号を監視して、ドアロック制御モードの設定を含む設定メニューのための特定のボタン操作がなされたか否か判別する（ステップＳ４１）。この例では、この特定のボタン操作としては、通常の使用者が行なわない操作とされており、例えばセキュリティボタン５１とメニューボタン５５との同時操作などとされている。このような特定のボタン操作は、ドアロック装置２の設置業者等が設定作業を行なうために定義されている。簡単に、ドアロック制御モードの設定変更ができないようにするためである。

ステップＳ４１で、前記の特定のボタン操作はされないと判別されたときには、単独のボタン操作に応じた処理などの、その他の処理を行なう（ステップＳ４２）。また、ステップＳ４１で、前記の特定のボタン操作がされたと判別されたときには、設定メニューの一覧をテレビ受像機７の画面に、前述の伝言記録再生の場合と同様にして表示するようにする（ステップＳ４３）。

この設定メニューの一覧表示に対しては、操作者は、行ないたい設定メニュー項目の選択をリモートコマンダ５０のカーソルキーを用いて行なう。ＣＰＵ２０１は、リモコン受信部３８の受信信号を監視してメニュー項目の選択操作がなされたか否か判別し（ステップＳ４４）、メニュー項目の選択操作がなされたと判別したときには、例えば反転表示して示す選択中項目を、選択操作に応じて変更する（ステップＳ４５）。

そして、設定項目の決定操作がなされたか否か判別する（ステップＳ４６）。また、ステップＳ４４で、メニュー項目の選択操作がなされないと判別したときには、即座にステップＳ４６に進んで設定項目の決定操作がなされたか否か判別する。

ステップＳ４６で、設定項目の決定操作がなされないと判別したときには、ステップＳ４４に戻る。また、ステップＳ４６で、設定項目の決定操作がなされたと判別したときには、選択された設定項目はドアロック制御モードの設定であるか否か判別し（ステップＳ４７）、そうではなかったときには選択された他の設定項目についての処理ルーチンを実行する（ステップＳ４８）。

ステップＳ４７で、選択された設定項目はドアロック制御モードの設定であると判別したときには、ＣＰＵ２０１は、テレビ受像機７の画面にオートロックモードと、逐次ロックモードとの選択画面を表示する（ステップＳ４９）。操作者は、この選択画面において、いずれかの選択入力をカーソルキー５６を用いて行なう。

そこで、ＣＰＵ２０１は、リモコン受信部３８を監視して、オートロックモードが選択されたか否か判別し（ステップＳ５０）、オートロックモードが選択されたと判別したときには、ドアロック装置２をオートロックモードに設定する設定動作を行なう（ステップＳ５１）。

すなわち、ＣＰＵ２０１は、監視制御装置３に内蔵の不揮発性メモリ部のドアロック装置２のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶すると共に、オートロックモードにする旨の指示をドアロック装置２に対して、ドアロック装置通信インターフェース２０６を通じて送る。

また、ステップＳ５０で、オートロックモードではないと判別したときには、ＣＰＵ２０１は、逐次ロックモードが選択されたと判別して、

ドアロック装置２を逐次ロックモードにする設定動作を行なう（ステップＳ５２）。

すなわち、ＣＰＵ２０１は、監視制御装置３に内蔵の不揮発性メモリ部のドアロック装置２のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶すると共に、逐次ロックモードにする旨の指示をドアロック装置２に対して、ドアロック装置通信インターフェース２０６を通じて送る。

以上で、監視制御装置３におけるロック制御モードの設定時の動作は終了となる。

次に、ドアロック装置通信インターフェース２０６を通じて送られてきたドアロック制御モードの指示情報を受信したドアロック制御装置１００の動作について、図２０のフローチャートを参照して説明する。

先ず、ドアロック制御装置１００のＣＰＵ１０１は、ドアロック制御モードの設定指示情報を監視制御装置３から受け取ったか否か判別し（ステップＳ６１）、受け取らないときには、その他の処理を行なう（ステップＳ６２）。

ステップＳ６１で、ドアロック制御モードの設定指示情報を監視制御装置３から受け取ったと判別したときには、ＣＰＵ１０１は、選択指示されたドアロック制御モードは、オートロックモードと逐次ロックモードのいずれであるか判別する（ステップＳ６３）。

ステップＳ６３で、選択指示されたドアロック制御モードはオートロックモードであると判別したときには、ＣＰＵ１０１は、ドアロック装置２のドアロック制御モードをオートロックモードに設定する処理を行なう（ステップＳ６４）。

すなわち、ステップＳ６４においては、ドアロック制御装置１００のＣＰＵ１０１は、オートロックモードの設定指示に基づき、ドアロック

装置２の内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとの両方をアクティブにし、かつ、プログラムＲＯＭ１３のドアロック制御のアプリケーションを、オートロックモード用のものとするようにする。そして、ＣＰＵ１０１は、ドアロック制御装置１００が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶する。

また、ステップＳ６３で、選択指示されたドアロック制御モードは逐次ロックモードであると判別したときには、ＣＰＵ１０１は、ドアロック装置２のドアロック制御モードを逐次ロックモードに設定する処理を行なう（ステップＳ６５）。

すなわち、ステップＳ６５においては、ドアロック制御装置１００のＣＰＵ１０１は、逐次ロックモードの設定指示に基づき、この例では、ドアロック装置２の内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとの両方をアクティブにし、かつ、プログラムＲＯＭ１３のドアロック制御のアプリケーションを、逐次ロックモード用のものとするようにする。そして、ＣＰＵ１０１は、ドアロック制御装置１００が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶する。

なお、この例では、逐次ロックモードにおいても、内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとの両方を用いるようにしたが、この逐次ロックモードにおいては、外側電子鍵リード／ライト部ｅｘのみをアクティブにして、内側電子鍵リード／ライト部２１ｉｎを用いないようにすることもできる。その場合には、家の内側からの施錠が問題になるが、例えば、内側からの玄関ドアの施錠を、電子鍵装置を用いずにマニュアル操作で行なえる構成とすればよい。

次に、オートロックモードと、逐次ロックモードのそれぞれの場合の

ドアロック装置２の動作について説明する。以下に説明するフローチャートにおける各ステップＳの動作は、ドアロック制御装置１００のＣＰＵ１０１が主として実行する処理動作である。

［オートロックモード；図２１～図２６］

オートロックモードのときの動作を、図２１～図２６のフローチャートを参照しながら説明する。このオートロックモードのときには、玄関ドア１は、定常状態では、施錠状態とされる。そして、電子鍵装置４０が、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘにかざされて通信が両者の間で行なわれ、識別情報、すなわち、電子鍵情報についての認証がとれたときには、所定時間のみ玄関ドアを開錠し、所定時間後に、自動的に玄関ドア１は施錠状態に戻るように、ドアロック制御装置１００により制御されるものである。

ＣＰＵ１０１は、インターフェース１０５，１０６を介して、内側電子鍵リード／ライト部２１ｉｎおよび外側電子鍵リード／ライト部２１ｅｘを監視し、電子鍵装置４０がかざされて、電子鍵装置４０と内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘとの間で通信が行われるのを待つ（ステップＳ７１）。

そして、ステップＳ７１において、ＩＣカード４０Ｆがかざされて、リード／ライト部２１ｉｎまたは２１ｅｘと通信が行なわれたと判別したときには、ＣＰＵ１０１は、識別情報をＩＣカード４０Ｆから受信し、例えばＲＡＭ１０４などに一時的に格納する（ステップＳ７２）。このとき、ドアロック制御装置１００が備える時計回路１２２の時刻情報も、通信があった時刻として、前記識別情報と共にＲＡＭ１０４に格納されると共に、当該時刻情報が、ＩＣカード４０Ｆに与えられ、制御用ＩＣ内４２のメモリに書き込まれる。

また、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード

／ライト部２１ｅｘのどちらと通信をしたかの情報として、通信相手のＩＤ等が制御用ＩＣ４２のメモリに書き込まれる。

次に、ＣＰＵ１０１は、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのどちらでＩＣカード４０Ｆと通信が行われたかを判別する（ステップＳ７３）。その判別結果と、前記の通信の時刻情報とは、家族情報メモリ１２０の、前記識別情報に対応する家人の記録エリアにも、通信履歴情報として書き込まれる。また、これらの識別情報、通信時刻、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのどちらでＩＣカード４０Ｆと通信が行われたかの判別結果は、監視制御装置３にも、その家族情報メモリ２０５に記憶させるために転送される。

［内側電子鍵リード／ライト部２１ｉｎでの通信の場合；図２１～図２３］

ステップＳ７３で、ＩＣカード４０Ｆと通信が行われたのが内側電子鍵リード／ライト部２１ｉｎであると判別したときには、ＣＰＵ１０１は、在宅者が外出する場合であるとして、以下のような処理を行なう。なお、この例では、在宅者が玄関ドア１を開錠し、玄関ドア１を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしている。

ＣＰＵ１０１は、先ず、家族情報メモリ１２０に記憶されている識別情報と、ＩＣカード４０Ｆから受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている電子鍵情報としての識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあるかどうかにより、当該ＩＣカード４０Ｆがドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該ＩＣカード４０Ｆについての認証を行なう（ステップＳ７４）。

そして、その認証結果を判別し（ステップＳ７５）、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを赤色で点滅させると共に、内側スピーカ２３ｉｎから警告音を放音して、認証ＮＧであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ７６）。そして、ドアロック機構２８は施錠状態のままとして、ステップＳ７１に戻る。

また、ステップＳ７５で、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを緑色で１秒間点灯させ、認証ＯＫであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ７７）。このとき、ＣＰＵ１０１により、併せて内側スピーカ２３ｉｎから「認証がとれました」というメッセージを放音させるようにしても良い。

そして、このとき、認証がＯＫであることから、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を開錠状態にし（ステップＳ７８）、内側スピーカ２３ｉｎから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ７９）。このとき、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させ、ドアロックの解除状態をＩＣカード４０Ｆの使用者に報知するようにしてもよい。

このとき、ＣＰＵ１０１は、ＩＣカード４０Ｆにより内側から玄関ドア１が開錠されたことを認識していることに基づき、当該ＩＣカード４０Ｆの使用者（在宅者）が外出しようとしていると認識する。そして、

監視制御装置３に対して窓の開閉状態についての問い合わせを送る（図２２のステップＳ８１）。

これに対して、監視制御装置３では、窓センサ６ａ，６ｂのセンサ出力をセンサハブ２０７を通じて取得して、窓の開閉を確認する。つまり、戸締りを確認する。そして、窓の開閉状態についての確認結果をドアロック装置インターフェース２０６を通じてドアロック制御装置１００に返信するようにする。

ドアロック制御装置１００では、この窓の開閉状態についての確認結果を、通信インターフェース１２１を通じて受信する（ステップＳ８２）。そして、ＣＰＵ１０１は、受信した当該確認結果を解析して、窓が開放されているか否か判別する（ステップＳ８３）。

そして、窓が開いていると判別したときには、ＣＰＵ１０１は、窓が開いていることを内側スピーカ２３ｉｎからの放音音声により警告する（ステップＳ８４）。また、窓が閉じていると判別したときには、ＣＰＵ１０１は、戸締りがＯＫであることを内側スピーカ２３ｉｎからの放音音声により報知する（ステップＳ８５）。

次に、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力をインターフェース１１１を通じて取り込み、玄関ドア１が開けられた否か監視する（ステップＳ８６）。そして、ＣＰＵ１０１は、玄関ドア１が開けられずに所定時間、例えば１０秒経過したかどうかを判別し（ステップＳ８７）、１０秒経過したと判別したときには、玄関ドア１を自動的に施錠状態に戻すようにする（ステップＳ８８）。そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを報知する（ステップＳ８９）。

また、ステップＳ８６で、ステップＳ７８での開錠後、１０秒以内に玄関ドア１が開かれたと判別したときには、ＣＰＵ１０１は、ステップ

Ｓ７２で取り込んだ識別情報で示される在宅者が外出をしたと認識して、当該識別情報、時刻情報を含む個人情報を、外出者情報として監視制御装置３に転送する（ステップＳ９０）。なお、このとき監視制御装置３に転送する情報には時刻情報を含めず、監視制御装置３がこれらの情報を受信した時刻を、時計回路２２１の時刻から認識するようにすることもできる。

その後、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力を参照して、玄関ドア１が閉じられたことを確認し（ステップＳ９１）、玄関ドア１が閉じられた後、所定時間、例えば３秒経過したことを確認したら（ステップＳ９２）、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を施錠状態に復帰させるようにする（図２３のステップＳ１０１）。そして、ＣＰＵ１０１は、外側ＬＥＤ２２ｅｘを緑色で点滅して、玄関ドア１が施錠状態に戻ったことをＩＣカード４０Ｆの使用者に報知する（ステップＳ１０２）。この外側ＬＥＤ２２ｅｘの緑色点滅は、所定時間、例えば１０秒間続けられる。

その後、ＣＰＵ１０１は、前記所定時間、例えば１０秒経過したか否か判別し（ステップＳ１０３）、所定時間経過していないと判別したときには、ステップＳ７１で通信が行われたと判別されたＩＣカード４０Ｆが、再度、外側電子鍵リード／ライト部２１ｅｘと通信したか否か判別する（ステップＳ１０４）、通信がなされないと判別したときにはステップＳ１０３に戻る。

そして、ステップＳ１０３で、ＩＣカード４０Ｆと外側電子鍵リード／ライト部２１ｅｘとで通信が行われずに、前記所定時間経過したと判別したときには、ＣＰＵ１０１は、内側電子鍵リード／ライト部２１ｉｎに対してＩＣカード４０Ｆがかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図２１のステップＳ７１に戻

る。

また、ステップＳ１０４で、玄関ドア施錠復帰後、外側ＬＥＤ２２ｅｘの緑色点滅が終了する所定時間経過する前に、ステップＳ７１において通信が行われたと判別されたＩＣカード４０Ｆと外側電子鍵リード／ライト部２１ｅｘとで通信が行われたと判別すると、ステップＳ１０１～Ｓ６３で確認された戸締りを再確認する（ステップＳ１０５）。

ステップＳ１０５で、戸締りがＯＫであると判別したときには、ＣＰＵ１０１は、通信インターフェース１２１を通じてセキュリティモードをオンにする要求を監視制御装置３に送信する（ステップＳ１０６）。

この要求に対しては、監視制御装置３は、そのときの在宅状況をチェックして、セキュリティレベルが図１５に示したいずれのレベルとなるかを判定する。そして、監視制御装置３は、その判定の結果、セキュリティレベルがレベルＤであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置１００に返し、セキュリティレベルがレベルＤ以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置１００に返す。

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップＳ１０７）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップＳ１０８）。

【０１９８】

また、ステップＳ１０７で、セキュリティモードがオンにできない旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１

は、外側スピーカ２３ｅｘから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップＳ１０９）。その後、ステップＳ７１に戻る。

また、ステップＳ１０５で、窓が開いていて戸締りが完了していないと判別したときには、ＣＰＵ１０１は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップＳ１１０）。そして、その後、ステップＳ７１に戻る。

［外側電子鍵リード／ライト部２１ｅｘでの通信の場合；図２４～図２６］

ステップＳ７１で、ＩＣカード４０Ｆと通信が行われたのが外側電子鍵リード／ライト部２１ｅｘであると判別したときには、ＣＰＵ１０１は、家人が帰宅した場合あるいはその他の外にいる者の入室要求であるとして、以下のような処理を行なう。

ＣＰＵ１０１は、まず、家族情報メモリ１２０に記憶されている識別情報と、ＩＣカード４０Ｆから受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあるかどうかにより、当該ＩＣカード４０Ｆがドアロック装置２に登録されたＩＣカード４０Ｆであるか否かを判別して、当該ＩＣカード４０Ｆについての認証を行なう（ステップＳ１２１）。

そして、その認証結果を判別し（ステップＳ１２２）、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを赤色で点滅させると共に、外

側スピーカ２３ｅｘから警告音を放音して、認証ＮＧであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１２３）。そして、ドアロック機構２８は施錠状態のままとして、ステップＳ７１に戻る。

また、ステップＳ１２２で、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを緑色で１秒間点灯させ、認証ＯＫであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１２４）。このとき、ＣＰＵ１０１により、合わせて外側スピーカ２３ｅｘから「認証がとれました」というメッセージを放音させるようにしても良い。

そして、このとき、認証がＯＫであることから、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を開錠状態にし（ステップＳ１２５）、外側スピーカ２３ｅｘから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ１２６）。このとき、外側ＬＥＤ２２ｅｘを、例えば緑色で点滅させ、ドアロックの解除状態をＩＣカード４０Ｆの使用者に報知するようにしてもよい。

次に、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力をインターフェース１１１を通じて取り込み、玄関ドア１が開けられた否か監視する（ステップＳ１２７）。そして、ＣＰＵ１０１は、玄関ドア１が開けられずに所定時間、例えば１０秒経過したかどうかを判別し（ステップＳ１２８）、１０秒経過したと判別したときには、玄関ドア１を自動的に施錠状態に戻すようにする（ステップＳ１２９）。そして、ＣＰＵ１０１は、外側ＬＥＤ２２ｅｘを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを報知する（ステップＳ１３０）。

その後、ＣＰＵ１０１は、所定時間、例えば１０秒経過したか否か判別し（ステップＳ１３１）、所定時間経過していないと判別したときには、ステップＳ７１で通信が行われたと判別された電子鍵装置が外側電子鍵リード／ライト部２１ｅｘと通信したか否か判別し（ステップＳ１３２）、通信がなされないと判別したときにはステップＳ１３１に戻る。

そして、ステップＳ１３１で、電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われずに、所定時間経過したと判別したときには、ＣＰＵ１０１は、外側電子鍵リード／ライト部２１ｅｘに対して電子鍵装置がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図２１のステップＳ７１に戻る。

また、ステップＳ１３２で、玄関ドア施錠復帰後、所定時間経過する前に、ステップＳ７１において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われたと判別すると、戸締りを確認する（ステップＳ１３３）。

このステップＳ１３３での戸締りの確認は、前述のステップＳ１２１～Ｓ１２３において説明した処理と同様に行なう。つまり、ドアロック制御装置１００は、監視制御装置３に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置３から取得する。そして、その問い合わせ結果から、戸締りがＯＫかどうかを判別する。

ステップＳ１３３で、戸締りがＯＫであると判別したときには、ＣＰＵ１０１は、通信インターフェース１２１を通じてセキュリティモードをオンにする要求を監視制御装置３に送信する（ステップＳ１３４）。

この要求に対しては、監視制御装置３は、そのときの在宅状況をチェックして、セキュリティレベルが図１５に示したいずれのレベルとなるかを判定する。そして、監視制御装置３は、その判定の結果、セキュリティレベルがレベルＤであるときには、セキュリティモードはオンにで

きないので、その旨をドアロック制御装置１００に返し、セキュリティレベルがレベルＤ以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置１００に返す。

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップＳ１３５）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップＳ１３６）。

また、ステップＳ１３５で、セキュリティモードがオンにできない旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップＳ１３７）。その後、ステップＳ７１に戻る。

また、ステップＳ１３３で、窓が開いていて戸締りが完了していないと判別したときには、ＣＰＵ１０１は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップＳ１３８）。そして、その後、ステップＳ７１に戻る。

ステップＳ１３１～ステップＳ１３８の処理は、一旦、玄関ドア１を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた者が、もう一度、室内に戻って、内側電子鍵リード／ライト部２１ｉｎに対して電子鍵装置をかざすところからやり直す手間を防止するための処理である。

すなわち、一旦、玄関ドア１を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた、あるいは失敗した場合に、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざして、玄関ドア１を一旦開錠させ、その後、１０秒待って再施錠になった後、１０秒以内に、再び、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざすことにより、セキュリティモードをオンにすることができるものである。このようにすれば、セキュリティモードをオンに設定するために、開錠してから室内に入り、内側電子鍵リード／ライト部２１ｉｎに電子鍵装置４０をかざすところからやり直す必要がなく、便利である。

次に、ステップＳ１２７で、ステップＳ１２５での開錠後、１０秒以内に玄関ドア１が開かれたと判別したときには、ＣＰＵ１０１は、ステップＳ７２で取り込んだ識別情報で示される外出者が帰宅したと認識して、当該識別情報、電子鍵装置と通信が行なわれた時刻情報を含む個人情報を、帰宅者情報として監視制御装置３に転送する（図２６のステップＳ１４１）。なお、このとき監視制御装置３に転送する情報には時刻情報を含めず、監視制御装置３がこれらの情報を受信した時刻を、時計回路２２１の時刻から認識するようにすることもできる。

その後、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力を参照して、玄関ドア１が閉じられたことを確認し（ステップＳ１４２）、玄関ドア１が閉じられた後、所定時間、例えば３秒経過したことを確認したら（ステップＳ１４３）、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を施錠状態に復帰させるようにする（ステップＳ１４４）。そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを報知する（ステップＳ１４５）。

その後、ＣＰＵ１０１は、帰宅者があったことから在宅状況が変更することに基づき、セキュリティレベルの変更指示を監視制御装置３に送る（ステップＳ１４６）。

このセキュリティレベルの変更指示を受け取った監視制御装置３では、ステップＳ１４１での帰宅者情報による在宅状況の変化を認識し、図１５に示した在宅状況とセキュリティレベルとの対応テーブルを参照して、セキュリティレベルの変更の必要があるか否か判別し、必要があるときには、セキュリティレベルを変更する。そして、監視制御装置３は、セキュリティレベルを変更したかどうかを、ドアロック制御装置１００に通知する。

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティレベルの変更に関する通知を受け取って（ステップＳ１４７）、セキュリティレベルが変更されたか否かを判別する（ステップＳ１４８）。

そして、ステップＳ１４８で、セキュリティモードが変更されたと判別したときには、ＣＰＵ１０１は、内側スピーカ２３ｉｎから、「セキュリティレベルを変更しました」というメッセージを放音する（ステップＳ１４９）。そして、ステップＳ７１に戻る。

なお、以上の説明では、帰宅者があったときには、ドアロック制御装置１００から、ステップＳ１４６において、監視制御装置３にセキュリティレベルの変更指示を送るようにしたが、監視制御装置３では、ステップＳ１４１での帰宅者情報の転送を受けるので、ドアロック制御装置１００からのセキュリティレベルの変更指示を受けなくても、自動的にセキュリティレベルの変更が必要かどうかを判断して、必要である場合には、セキュリティレベルを自動的に変更するようにしても良い。その場合には、セキュリティレベルを変更したときには、その旨をドアロッ

ク制御装置１００に転送するようにする。

［逐次ロックモードの説明；図２７～図２９］

次に、逐次ロックモードのときの動作を、図２７～図２９のフローチャートを参照しながら説明する。この逐次ロックモードのときには、ＩＣカード４０Ｃが、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘにかざされて通信が両者の間で行なわれ、電子鍵情報としての識別情報についての認証がとれたときには、そのときの玄関ドア１の開錠あるいは施錠の状態とは逆の状態になるように、ドアロック機構２８は、ドアロック制御装置１００により制御されるものである。

ＣＰＵ１０１は、インターフェース１０５，１０６を介して、内側電子鍵リード／ライト部２１ｉｎおよび外側電子鍵リード／ライト部２１ｅｘを監視し、ＩＣカード４０Ｃがかざされて、ＩＣカード４０Ｃと内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘとの間で通信が行われるのを待つ（ステップＳ１５１）。

そして、ステップＳ１５１において、ＩＣカード４０Ｆがかざされて、ＩＣカード４０Ｆと通信が行なわれたと判別したときには、ＣＰＵ１０１は、識別情報をＩＣカード４０Ｆから受信し、例えばＲＡＭ１０４などに一時的に格納する（ステップＳ１５２）。このとき、前述と同様に、ＩＣカード４０Ｆには時刻情報等が書き込まれると共に、家族情報メモリ１２０および監視制御装置３の家族情報メモリ２０５への時刻情報等の書き込みが行なわれる。

内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのどちらでＩＣカード４０Ｆと通信が行われたかを判別する（ステップＳ１５３）。

［内側電子鍵リード／ライト部２１ｉｎでの通信の場合；図２７］

ステップＳ１５３で、ＩＣカード４０Ｆと通信が行われたのが内側電子鍵リード／ライト部２１ｉｎであると判別したときには、ＣＰＵ１０１は、在宅者が外出する場合あるいは玄関ドア１をセキュリティのために施錠する場合であるとして、以下のような処理を行なう。

ＣＰＵ１０１は、先ず、家族情報メモリ１２０に記憶されている識別情報と、ＩＣカード４０Ｆから受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあるかどうかにより、当該ＩＣカード４０Ｆがドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該ＩＣカード４０Ｆについての認証を行なう（ステップＳ１５４）。

そして、その認証結果を判別し（ステップＳ１５５）、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを赤色で点滅させると共に、内側スピーカ２３ｉｎから警告音を放音して、認証ＮＧであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１５６）。そして、ドアロック機構２８は、その前の状態のままとして、ステップＳ１５１に戻る。

また、ステップＳ１５５で、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを緑色で１秒間点灯させ、認証ＯＫであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１５７）。このとき、ＣＰＵ１０１により、併せて内側

スピーカ２３ｉｎから「認証がとれました」というメッセージを放音させるようにしても良い。

そして、ＣＰＵ１０１は、現在のドアロック機構２８による玄関ドア１のロック状態は、施錠状態になっているか否か判別する（ステップＳ１５８）。このステップＳ１５８で、ドアロック機構２８による玄関ドア１のロック状態が、開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部１１２を駆動制御する（ステップＳ１５９）。

そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことをＩＣカード４０Ｆの使用者に報知するようにする（ステップＳ１６０）。

そして、ＣＰＵ１０１は、ステップＳ１５２で取り込んだ識別情報で示される者が、セキュリティのために施錠をしたと認識して、当該識別情報を含む個人情報を、在宅者情報として監視制御装置３に転送する（ステップＳ１６１）。

また、ステップＳ１５８で、現在のドアロック機構２８のロック状態は、施錠状態であると判別したときには、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８を開錠状態にし（ステップＳ１６２）、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ１６３）。

そして、このときには、ＣＰＵ１０１は、ステップＳ１５２で取り込んだ識別情報で示される者が、開錠をして外出をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置３に転送する（ステップＳ１６４）。

[外側電子鍵リード／ライト部２１ｅｘでの通信の場合；図２８～図２９]

ステップＳ１５３で、ＩＣカード４０Ｆと通信が行われたのが外側電子鍵リード／ライト部２１ｅｘであると判別したときには、ＣＰＵ１０１は、家人が帰宅して開錠する場合あるいは家人が外出のため施錠する場合であるとして、以下のような処理を行なう。

ＣＰＵ１０１は、まず、家族情報メモリ１２０に記憶されている識別情報と、ＩＣカード４０Ｆから受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあるかどうかにより、当該ＩＣカード４０Ｆがドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該ＩＣカード４０Ｆについての認証を行なう（ステップＳ１７１）。

そして、その認証結果を判別し（ステップＳ１７２）、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを赤色で点滅させると共に、外側スピーカ２３ｅｘから警告音を放音して、認証ＮＧであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１７３）。そして、ドアロック機構２８は施錠状態のままとして、ステップＳ１５１に戻る。

また、ステップＳ１７２で、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを緑色で１秒間点灯させ、認証ＯＫであることをＩＣカード４０Ｆの使用者に報知す

る（ステップＳ１７４）。このとき、ＣＰＵ１０１により、併せて外側スピーカ２３ｅｘから「認証がとれました」というメッセージを放音させるようにしても良い。

そして、ＣＰＵ１０１は、現在のドアロック機構２８のロック状態は、施錠状態になっているか否か判別する（ステップＳ１７５）。このステップＳ１７５で、現在のドアロック機構２８による玄関ドア１のロック状態は、施錠状態であると判別したときには、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を開錠状態にし（ステップＳ１７６）、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ１７７）。

そして、ＣＰＵ１０１は、ステップＳ１５２で取り込んだ識別情報で示される者が、帰宅のため開錠をしたと認識して、当該識別情報および帰宅時刻情報（電子鍵装置と通信が行なわれた時刻）を含む個人情報を、帰宅者情報として監視制御装置３に転送する（ステップＳ１７８）。この場合にも、前述と同様にして、監視制御装置３がこれらの情報を受信した時刻を、時計回路２２１の時刻から認識して、その時刻を帰宅時刻とするようにしてもよい。

また、ステップＳ１７５で、現在の玄関ドア１のロック状態が開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を施錠状態にする（ステップＳ１７９）。

そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことをＩＣカード４０Ｆ

の使用者に報知するようにする（ステップＳ１８０）。

そして、ＣＰＵ１０１は、ステップＳ１５２で取り込んだ識別情報で示される者が、外出のために施錠をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置３に転送する（ステップＳ１８１）。

そして、施錠後、ＣＰＵ１０１は、所定時間、例えば１０秒経過したか否か判別し（図２９のステップＳ１８２）、所定時間経過していないと判別したときには、ステップＳ１７１で通信が行われたと判別されたＩＣカード４０Ｆが、再度、外側電子鍵リード／ライト部２１ｅｘと通信したか否か判別し（ステップＳ１８３）、通信がなされないと判別したときにはステップＳ１８２に戻る。

また、ステップＳ１８３で、玄関ドア施錠後、所定時間経過する前に、ステップＳ７１において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われたと判別すると、戸締りを確認する（ステップＳ１８４）。

このステップＳ１８４での戸締りの確認は、前述のステップＳ１０１～Ｓ１０３において説明した処理と同様に行なう。つまり、ドアロック制御装置１００は、監視制御装置３に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置３から取得する。そして、その問い合わせ結果から、戸締りがＯＫかどうかを判別する。

ステップＳ１８４で、戸締りがＯＫであると判別したときには、ＣＰＵ１０１は、通信インターフェース１２１を通じてセキュリティモードをオンにする要求を監視制御装置３に送信する（ステップＳ１８５）。

この要求に対しては、監視制御装置３は、そのときの在宅状況をチェックして、セキュリティレベルが図１５に示したいずれのレベルとなるかを判定する。そして、監視制御装置３は、その判定の結果、セキュリ

ティレベルがレベルＤであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置１００に返し、セキュリティレベルがレベルＤ以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置１００に返す。

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップＳ１８６）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップＳ１８７）。

また、ステップＳ１８６で、セキュリティモードがオンにできない旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップＳ１８８）。その後、ステップＳ１５１に戻る。

また、ステップＳ１８４で、窓が開いていて戸締りが完了していないと判別したときには、ＣＰＵ１０１は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップＳ１８９）。そして、その後、ステップＳ１７１に戻る。

［監視制御装置３におけるセキュリティ動作；図３０］

上述のようにして、監視制御装置３は、ドアロック制御装置１００からの指示を受けてセキュリティモードをオンにするが、リモートコマンダ５０のセキュリティボタン５１を押すことによってもセキュリティモードをオンにすることができる。そして、監視制御装置３のセキュリテ

ィモードオン状態は、リモートコマンダ５０のオフボタン５２を操作すると、オフとすることができる。

図３０は、リモートコマンダ５０を操作することにより、監視制御装置３のセキュリティモードのオン・オフを制御する動作を説明するためのフローチャートである。

まず、ＣＰＵ２０１は、リモートコマンダ５０からの遠隔操作信号を監視して、リモートコマンダ５０で操作入力がなされたか否か判別する（ステップＳ１９１）。そして、操作入力がなされたと判別したときには、ＣＰＵ２０１は、操作されたのはセキュリティボタン５１であるか否か判別する（ステップＳ１９２）。

ステップＳ１９２での判別の結果、セキュリティボタン５１の操作であると判別したときには、ＣＰＵ２０１は、リモコン送信部３９から電源オンのリモコン信号をテレビ受像機７のリモコン受信部に送り、テレビ受像機７をオンにする（ステップＳ１９３）。

そして、ＣＰＵ２０１は、ＲＯＭ２０３から読み出したデータに基づいて生成した画像情報を、テレビインターフェース２１７を通じてテレビ受像機７に送り、テレビ受像機７の画面にセキュリティモードオンの確認画面を表示する（ステップＳ１９４）。その後、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７の電源をオフするリモコン信号を送出して、テレビ受像機７をオフさせる（ステップＳ１９５）。

そして、ＣＰＵ２０１は、その所定時間、例えば５分経過後（ステップＳ１９６）、セキュリティモードをオンにして（ステップＳ１９７）、セキュリティ監視動作を実行する（ステップＳ１９８）。ステップＳ１９６における所定時間は、セキュリティボタン５１を操作した使用者が、セキュリティモードオンに設定した後、玄関ドアから退出するまでの時間を考慮した時間とされている。

ステップＳ１９２において、リモートコマンダ５０で操作されたボタンがセキュリティボタン５１ではないと判別したときには、ＣＰＵ２０１は、操作されたのはオフボタン５２であるか否か判別する（ステップＳ１９９）。このステップＳ１９９でオフボタン５２ではないと判別したときには、ＣＰＵ２０１は、その他のボタンが押されたことによる処理を実行する（ステップＳ２００）。

ステップＳ１９９での判別の結果、オフボタン５２であると判別したときには、ＣＰＵ２０１は、リモコン送信部３９から電源オンのリモコン信号をテレビ受像機７のリモコン受信部に送り、テレビ受像機７をオンにする（ステップＳ２０１）。

そして、ＣＰＵ２０１は、ＲＯＭ２０３から読み出したデータに基づいて生成した画像情報を、テレビインターフェース２１７を通じてテレビ受像機７に送り、テレビ受像機７の画面にセキュリティモードオフの確認画面を表示する（ステップＳ２０２）。その後、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７の電源をオフするリモコン信号を送出して、テレビ受像機７をオフさせる（ステップＳ２０３）。

そして、ＣＰＵ２０１は、セキュリティモードをオフにする処理を行なう（ステップＳ２０４）。以上で、図３０の処理ルーチンは終了となる。

［セキュリティモードオンにおける監視動作］

図３１および図３２は、監視制御装置３において、セキュリティモードオンとされたときの処理動作である。これは、前述のリモートコマンダ５０でのセキュリティボタン５１の操作時に起動されるもので、このときのセキュリティレベルは、レベルＡの場合である。なお、ドアロック制御装置１００からのセキュリティモードオン指示があったときには、前述したように、在宅者の状況が参酌されてセキュリティレベルが決定

され、その決定されたセキュリティレベルでセキュリティモードがオンとされるものである。

図３１においては、先ず、ＣＰＵ２０１は、ビデオカメラ３１の撮影画像の取り込みを開始する（ステップＳ２１１）。このとき、マイクロホン３４で収音した音声も一緒に取り込みを行なう。前述したように、画像・音声メモリ２０８に設けられるセキュリティモード用の監視情報領域は、リングバッファ形式とされており、この例では、最新の３０秒分の画像・音声情報が常に画像・音声メモリ２０８に格納されるようにされている。監視カメラ１３からの撮影画像についても同様にされている。

次に、ＣＰＵ２０１は、センサハブ２０７からの窓センサ１６ａ、１６ｂのセンサ出力と、玄関ドア１のドア開閉センサ２７のセンサ出力の監視を開始するように制御する（ステップＳ２１２）。さらに、ＣＰＵ２０１は、火災センサ４およびガスセンサ５のセンサ出力の監視を開始するように制御する（ステップＳ２１３）。監視カメラ１３は、火災センサ４やガスセンサ５のオン・オフに応じてオン・オフする。

次に、ＣＰＵ２０１は、人感センサ３３のセンサ出力を監視して、侵入者がないかどうかチェックする（ステップＳ２１４）。侵入者なしと判別したときには、窓センサ１６ａ，１６ｂのセンサ出力や、ドア開閉センサ２７のセンサ出力から、異常を検知したか否か判別する（図３２のステップＳ２３１）。

ステップＳ２３１で、異常を検知しないと判別したときには、ＣＰＵ２０１は、火災センサ４やガスセンサ５のセンサ出力から、異常を検知したか否か判別する（ステップＳ２３２）。ステップＳ２３２で、異常を検知しないと判別したときには、ステップＳ２１４に戻る。

そして、ステップＳ２１４で、侵入者を人感センサ３３により検知し

たと判別したときには、ＣＰＵ２０１は、照明機構３２０を制御して、照明３２をオンにする（ステップＳ２１５）。そして、侵入者の検知時点の１０秒前から、検知時点の２０秒後までの３０秒分の画像・音声情報を、画像・音声メモリ２０８から読み出し、１回目の画像として、管理サーバ装置１０に転送する（ステップＳ２１６）。管理サーバ装置１０では、この転送されてきた画像・音声情報により、侵入者を認識して、適切な処置を取ることができる。

次に、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７に電源オンのリモコン信号を送り、テレビ受像機７をオンにする（ステップＳ２１７）。そして、ＣＰＵ２０１は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機７に送り、それら威嚇画像および威嚇音声を出力する（ステップＳ２１８）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

次に、ＣＰＵ２０１は、監視制御装置３に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップＳ２１９）。

そして、ＣＰＵ２０１は、その後、数秒間隔で、画像・音声メモリ２０８のリングバッファに格納されている３０秒分の画像・音声情報を繰り返し管理サーバ装置１０に転送する（ステップＳ２２０）。そして、ＣＰＵ２０１は、人感センサ３３が侵入者を検知しなくなったか否か判別し（ステップＳ２２１）、検知しなくなるまで、３０秒分の画像・音声情報を管理サーバ装置１０に転送する処理作業を継続する。

そして、ＣＰＵ２０１は、人感センサ３３が侵入者を検知しなくなったと判別したときには、３０秒分の画像・音声情報の管理サーバ装置１０への転送を中止する（ステップＳ２２２）。そして、ステップＳ２３１に戻って、セキュリティ監視を続ける。

また、ステップＳ２３１において、異常を検知したと判別したときには、ＣＰＵ２０１は、窓センサ６ａ，６ｂやドア開閉センサ２７の近傍に設置されている監視カメラ１３からの検知時点の１０秒前から、検知時点の２０秒後までの３０秒分画像を１回目として、管理サーバ装置１０に転送する（ステップＳ２３４）。

そして、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７に電源オンのリモコン信号を送り、テレビ受像機７をオンにする（ステップＳ２３５）。そして、ＣＰＵ２０１は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機７に送り、それら威嚇画像および威嚇音声を出力する（ステップＳ２３６）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

次に、ＣＰＵ２０１は、監視制御装置３に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップＳ２３７）。

そして、ＣＰＵ２０１は、その後、数秒間隔で、画像・音声メモリ２０８のリングバッファに格納されている３０秒分の画像・音声情報を繰り返し管理サーバ装置１０に転送する（ステップＳ２３８）。そして、ＣＰＵ２０１は、リモートコマンダ５０のオフボタン５２によるオフ指示を待ち（ステップＳ２３９）、オフ指示が有ったときには、セキュリティモードをオフとする。

また、ステップＳ２３２で、火災センサ４またはガスセンサ５で異常が検知されたと判別したときには、ＣＰＵ２０１は、監視制御装置３に設定登録されている、例えば警備会社、消防署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップＳ２３３）。そして、ステップＳ２３９に進む。

なお、画像・音声情報を監視制御装置３から受け取った管理サーバ装

置１０は、Ｗｅｂページにそれらの画像・音声情報を載せる。そこで、監視制御装置３から連絡を受け取った携帯電話の持ち主は、管理サーバ装置１０の当該Ｗｅｂページにアクセスして、どのような異常が発生したかを知ることができ、適切な対応処置を講じることが可能になる。

［監視制御装置３におけるドアロック制御装置１００からの指示による連携；図３３］

監視制御装置３のＣＰＵ２０１は、ドアロック制御装置１００から受け取った情報や指示に応じて、図３３に示すような連携動作を行なう。なお、この例は、セキュリティレベルの変更は、ＣＰＵ２０１が、ドアロック制御装置１００からの変更指示を受けて行なうのではなく、ドアロック制御装置１００からの個人情報を受け取った結果による在宅状況の変化をチェックして、必要に応じて行なうようにした場合である。

すなわち、ＣＰＵ２０１は、ドアロック制御装置１００からセキュリティモードオンの指示を受け取ったか否か判別する（ステップＳ２４１）。受け取らないと判別したときには、ＣＰＵ２０１は、その他の処理を行なう（ステップＳ２４２）。

ステップＳ２４１でセキュリティモードオンの指示を受信したと判別したときには、ＣＰＵ２０１は、家族情報メモリ２０５の記憶情報を参照して、在宅状況をチェックする（ステップＳ２４３）。そして、図１５に示したテーブルを参照して、在宅状況に応じたセキュリティレベルを認識し、セキュリティモードオンにすることが可能であるか否か判別する（ステップＳ２４４）。

ステップＳ２４４で、セキュリティモードオンにすることができないと判別したときには、ＣＰＵ２０１は、その旨をドアロック制御装置１００に通知する（ステップＳ２４５）。

一方、ステップＳ２４４で、セキュリティモードオンにすることが可

能であると判別したときには、セキュリティモードをオンにすることができる旨をドアロック制御装置１００に通知し（ステップＳ２４６）、所定時間経過するのを待つ（ステップＳ２４７）。

所定時間経過したことを確認したら、ＣＰＵ２０１は、在宅状況に応じたセキュリティレベルでセキュリティモードをオンにする（ステップＳ２４８）。そして、セキュリティ監視動作を開始する（ステップＳ２４９）。

このセキュリティ監視動作中において、ドアロック制御装置１００から識別情報を含む個人情報を受信したか否か判別し(ステップＳ２５０)、受信しなければステップＳ２４９に戻って、セキュリティ監視動作を継続する。ドアロック制御装置１００から個人情報を受信したと判別したときには、その結果としての在宅状況の変化をチェックし（ステップＳ２５１）、セキュリティレベルの変更が必要であるか判別する（ステップＳ２５２）。

セキュリティレベルの変更が必要ではないと判別したときには、ＣＰＵ２０１は、ステップＳ２４９に戻って、セキュリティ監視動作を継続する。また、ステップＳ２５２で、セキュリティレベルの変更が必要であると判別したときには、変更の結果、セキュリティモードはオフにすべきものであるか否か判別し（ステップＳ２５３）、そうではないときには、在宅状況に応じてセキュリティレベルを変更する（ステップＳ２５４）。そして、セキュリティレベルを変更した旨をドアロック制御装置１００に通知する（ステップＳ２５５）。

また、ステップＳ２５３で、セキュリティモードはオフにすべきものであると判別したときには、セキュリティモードをオフにし（ステップＳ２５６）、その旨をドアロック制御装置１００に通知する（ステップＳ２５７）。そして、ステップＳ２４１に戻る。

以上のようにして、この実施形態によれば、非接触の電子鍵装置を用いて、施錠、開錠を行なうので、鍵穴がなく、いわゆるピッキング対策の防犯効果がある。

また、電子鍵装置の所有者の生体情報により、電子鍵装置において、当該電子鍵装置の使用者が所有者であるか否かについてのチェック（認証）を行ない、認証がＯＫであるときにのみ、電子鍵情報を送出するようにするので、電子鍵装置を紛失したとしても、所有者以外が電子鍵装置を使用して、ドアロック制御をすることは不可能であるので、セキュリティ上の安全性が非常に高い。

また、ドアロック装置２を、オートロックモードと、逐次ロックモードとで使い分けることができるので、使用者が、自分の使い勝ってに合わせて、いずれのモードにするかを選択することができて、非常に便利である。

また、内側電子鍵リード／ライト部２１ｉｎを設けて、この内側電子鍵リード／ライト部２１ｉｎによっても、ドアのロック状態を電子鍵装置により制御することができるので、窓などから侵入した不審者が玄関ドアから退出するのを妨げることができる。

また、内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとを設けることにより、これらと電子鍵装置との通信により、家族の入退出の管理をすることが容易である。

そのため、ドアロック装置２と、監視制御装置３とを組み合わせることにより、効率的なセキュリティ管理をすることができるようになる。そして、セキュリティモードをドアロック時に設定できるようにしているので、従来は、家の中で設定して、所定時間後に、家の外に出なければならないなどのあわただしさを解消することができる。

また、窓の閉め忘れがあったときには、ドアの開閉時に確認されるの

で、窓の閉め忘れを防止することができる。

また、家人の年齢、性別などにより、セキュリティモードのレベルを可変することができるようにしたので、在宅者が弱者である場合にも効果的なセキュリティレベルを設定することができる。また、ドアロックの開錠、施錠に連携して、在宅状況の変化を把握することにより、セキュリティレベルの変更をすることができるというメリットもある。

［電子鍵情報の登録］

この電子鍵情報としての識別情報の登録が簡単にできることはセキュリティの点で好ましくないので、この例では、この電子鍵情報としての識別情報の登録は、次のようにセキュリティを重視した方法により、例えばドアロック装置２の販売業者あるいは設置業者もしくは使用者により行なわれる。

先ず、本鍵情報の登録について説明する。この実施形態においては、前述したように、初期的な本鍵情報となる識別情報を記憶する電子鍵装置は、ＩＣカードとしており、ドアロック装置２の販売業者あるいは設置業者から、ドアロック装置２の各戸への設置に際して、使用者に渡される。

この実施形態の場合、ドアロック装置２の各戸への設置前に、当該ドアロック装置２を設置する戸の家族構成員の各人についての個人情報が収集される。そして、当該家族構成員の各人に対して、本鍵情報となる識別情報を記憶するＩＣカードが割り当てられ、それぞれのＩＣカードに記憶される本鍵情報としての識別情報と、前記収集された個人情報とからなる個人プロファイル情報が構成される。

そして、設置されるドアロック装置２のシリアル番号等からなる製品番号、設置される住所、電話番号、ドアロック装置を利用する家族構成員の氏名などのユーザ情報と、各家族構成員の前記個人プロファイル情

報が、予め管理サーバ装置１０のドアロック装置管理データベース３０５に、記憶される。すなわち、家族構成員それぞれの本鍵情報は、各家族構成員の個人プロファイル情報に含められて予め管理サーバ装置１０に登録されている。

この際に、ドアロック装置管理データベースにおいては、家族構成員の個人プロファイル情報は、監視制御装置３の通信ネットワーク上のアドレス情報に対応して記憶される。当該アドレス情報としては、前述したように、この例では、電話番号やＩＰアドレスが用いられる。

管理サーバ装置１０に登録された本鍵情報および各家族構成員の個人プロファイル情報は、ドアロック装置２の設置業者や販売業者が、ドアロック装置２の設置を完了したときに、管理会社の管理サーバ装置１０に初期登録要求をしたときに、管理サーバ装置１０から監視制御装置３に転送されることにより、監視制御装置３の家族情報メモリ２０５に書き込まれて登録される。また、監視制御装置３に登録された情報のうち、少なくとも本鍵情報は、ドアロック制御装置１００に転送されることにより、その家族情報メモリ１２０登録される。

図３４は、初期登録要求を受けたときの管理サーバ装置１０の動作を示すものである。図３４の各ステップの動作は、主としてＣＰＵ３０１が主体となって行なうものである。

先ず、ＣＰＵ３０１は、初期登録要求を受け付けたか否か判別する（ステップＳ２６１）。この初期登録要求は、ドアロック装置２のシリアル番号等の装置識別情報を伴ったものとされているもので、例えばパーソナルコンピュータなどから通信ネットワークを通じて管理サーバ装置１０に送られる場合と、電話等で、初期登録要求を受けたオペレータが図示しない入力手段により入力する場合とがある。

ＣＰＵ３０１は、この初期登録要求を受け取ると、装置識別情報を検

索子として、ドアロック装置データベースを検索し、予め登録されているドアロック装置２および監視制御装置３の通信ネットワーク９上でのアドレス情報を読み出して、初期登録要求を含む発呼をする。つまり、初期登録要求されたドアロック装置２が接続されている監視制御装置３に対して初期登録要求の発呼を行なう（ステップＳ２６２）。

このとき、監視制御装置３は、自動応答を行なうので、ＣＰＵ３０１は、当該監視制御装置３からの応答を確認して、当該監視制御装置３との間に通信路を形成する（ステップＳ２６３）。

次に、ＣＰＵ３０１は、ドアロック装置２に関連して上述のように管理サーバ装置１０のドアロック装置データベース２０５に記憶している、ドアロック装置が設置された家の家族構成員全員についての本鍵情報を含む個人プロファイル情報を監視制御装置３に送信する（ステップＳ２６４）。

次に、ＣＰＵ３０１は、監視制御装置３に送信すべき情報が全部終了し終わり、監視制御装置３から登録完了通知が到来するのを待ち（ステップＳ２６５）、登録完了通知を受け取ったと判別したときには、監視制御装置３との通信路を切断して（ステップＳ２６６）、この初期登録の処理ルーチンを終了する。

この初期登録要求情報を受け取る監視制御装置３の動作を、図３５のフローチャートを参照して説明する。

監視制御装置３のＣＰＵ２０１は、管理サーバ装置１０からの着信を受信したか否か判別し（ステップＳ２７１）、管理サーバ装置１０からの着信の受信でなかったと判別したときには、その他の処理を行なう（ステップＳ２７２）。

管理サーバ装置１０からの着信を受信したと判別したときには、ＣＰＵ２０１は、その着信に自動応答して管理サーバ装置１０との間に通信

路を形成する（ステップＳ２７３）。そして、受信した着信は初期登録要求であるか否か判別する（ステップＳ２７４）。初期登録要求であると判別すると、ＣＰＵ２０１は、管理サーバ装置１０からの登録情報を待ち、登録情報を受信したら（ステップＳ２７５）、受信した登録情報を、家族情報メモリ２０５に書き込む（ステップＳ２７６）。

そして、家族全員についての登録情報の書き込みが完了したら、管理サーバ装置１０に登録完了通知を返送し（ステップＳ２７７）、管理サーバ装置１０との通信路を切断する（ステップＳ２７８）。

次に、ＣＰＵ２０１は、家族情報メモリ２０５に書き込んで登録した個人プロファイル情報のうち、少なくとも家族構成員のそれぞれについての本鍵情報である識別情報をドアロック制御装置１００に転送する（ステップＳ２７９）。ドアロック制御装置１００は、この情報を受けて、家族情報メモリ１２０に受信した本鍵情報を登録する。本鍵情報としての識別情報のほかに、家族構成員についての個人情報の必要なものをも、ドアロック制御装置１００に転送するようにしてもよいことは言うまでもない。なお、ドアロック制御装置１００での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

そして、ＣＰＵ２０１は、ドアロック制御装置１００への本鍵情報および必要は情報の転送の終了を確認すると（ステップＳ２８０）、この処理ルーチンを終了する。

なお、ステップＳ２７４で、初期登録ではないと判別したときには、ＣＰＵ２０１は、バックアップ鍵の登録要求であるか否か判別し（ステップＳ２８１）、バックアップ鍵の登録要求であると判別したときには、当該バックアップ登録の処理を実行する（ステップＳ２８２）。このバックアップ登録の処理の詳細説明はこの明細書では省略する。

また、ステップＳ２８１でバックアップ登録要求ではないと判別した

ときには、ＣＰＵ２０１は、紛失鍵の抹消要求であるか否か判別する（ステップＳ２８３）。そして、紛失鍵の抹消要求でないと判別したときには、ＣＰＵ２０１は、その他の処理を実行し（ステップＳ２８４）、紛失鍵の抹消要求であると判別したときには、当該抹消要求の処理を実行する（ステップＳ２８５）。この抹消処理についての詳細説明はこの明細書では省略する。以上で、図３５の処理を終了する。

［通知連絡設定］

次に、この実施形態では、ユーザは、監視制御装置３に対して、予め、帰宅予定者、外出予定者、帰宅予定時刻、外出予定時刻、通知連絡者などを設定することができ、監視制御装置３は、それら設定された情報を通知連絡設定メモリ２２２に記憶する。そして、後述するように、監視制御装置３は、設定された帰宅予定時刻や外出予定時刻を監視して、設定された帰宅予定者、設定された外出予定者、設定された通知連絡者に、当該帰宅予定者、当該外出予定者の入退出に関する情報、つまり、帰宅、外出に関する情報を通知連絡するようにする。

先ず、帰宅予定者、外出予定者、帰宅予定時刻、外出予定時刻、通知連絡者などの設定処理について、図３６および図３７のフローチャートを参照して説明する。

先ず、監視制御装置３のＣＰＵ２０１は、リモコン受信部３８の受信信号を監視して、リモートコマンダ５０でボタン操作されたか否か判別する（ステップＳ２９１）。このステップＳ２９１で、ボタン操作されないと判別されたときには、その他の処理を行なう（ステップＳ２９２）。

ステップＳ２９１で、リモートコマンダ５０でボタン操作がされたと判別したときには、ＣＰＵ２０１は、リモートコマンダ５０で操作されたボタンは、メニューボタン５５であるか否か判別する（ステップＳ２９３）。メニューボタン５５ではないと判別したときには、ＣＰＵ２０

１は、操作されたボタンに対応する処理を実行する（ステップＳ２９４）。

また、ステップＳ２９３で、操作されたボタンがメニューボタン５５であると判別したときには、ＣＰＵ２０１は、テレビ受像機７に電源が投入されていないときには、テレビ受像機７の電源をオンにして（ステップＳ２９５）、メニューの一覧をテレビ受像機７の画面に、前述の伝言記録再生の場合と同様にして表示するようにする（ステップＳ２９６）。

このメニューの一覧表示に対しては、操作者は、行ないたい設定メニュー項目の選択をリモートコマンダ５０のカーソルキーを用いて行なう。ＣＰＵ２０１は、リモコン受信部３８の受信信号を監視してメニュー項目の選択操作がなされたか否か判別し（ステップＳ２９７）、メニュー項目の選択操作がなされたと判別したときには、例えば反転表示して示す選択中項目を、選択操作に応じて変更する（ステップＳ２９８）。そして、設定項目の決定操作がなされたか否か判別する（ステップＳ２９９）。

また、ステップＳ２９７で、メニュー項目の選択操作がなされないと判別したときには、ＣＰＵ２０１は、即座にステップＳ２９９に進んで設定項目の決定操作がなされたか否か判別する。そして、ステップＳ２９９で、設定項目の決定操作がなされないと判別したときには、ステップＳ２９７に戻る。

また、ステップＳ２９９で、設定項目の決定操作がなされたと判別したときには、ＣＰＵ２０１は、選択された設定項目は帰宅予定に関する通知の設定であるか否か判別し（図３７のステップＳ３０１）、そうではなかったときには選択された設定項目は外出予定に関する通知の設定であるか否か判別する（ステップＳ３０３）。そして、外出予定に関する通知の設定ではないと判別したときには、その他の設定項目についての処理ルーチンを実行する（ステップＳ３０５）。

ステップＳ３０１で、帰宅予定に関する通知の設定であると判別したときには、ＣＰＵ２０１は、帰宅予定時刻、帰宅予定者、帰宅通知連絡者などの設定用画面をテレビ受像機７の画面に表示する（ステップＳ３０２）。この例の場合、設定用画面においてユーザに対して設定要求される帰宅通知連絡者は、帰宅予定者本人以外とされる。しかし、後述するように、帰宅予定に関する通知の設定がなされた場合には、監視制御装置３では、帰宅予定時刻になっても帰宅しない帰宅予定者に帰宅を促す通知を帰宅予定者に送るようにするので、実際の帰宅通知連絡者には、当該帰宅予定者本人が予め含まれるものとなる。

ステップＳ３０２の次のステップＳ３０６において、ＣＰＵ２０１は、帰宅予定に関する通知について、すべての設定項目の設定入力が終了したか否か判別し（ステップＳ３０６）、すべての設定入力が終了したと判別したときには、設定された項目情報を、通知連絡設定メモリ２２２に書き込み（ステップＳ３０７）、その後、テレビ受像機７の電源をオフして（ステップＳ３０８）、この設定処理ルーチンを終了する。

また、ステップＳ３０３で、外出予定に関する通知の設定であると判別したときには、ＣＰＵ２０１は、外出予定時刻、外出予定者、外出通知連絡者などの設定用画面をテレビ受像機７の画面に表示する（ステップＳ３０４）。この例の場合、設定用画面においてユーザに設定要求される外出通知連絡者は、外出予定者本人以外とされる。しかし、後述するように、外出予定に関する通知の設定がなされた場合には、監視制御装置３では、外出予定時刻になっても外出しない外出予定者に外出を促す通知を外出予定者に送るようにするので、実際の外出通知連絡者には、当該外出予定者本人が予め含まれるものとなる。

そして、ステップＳ３０４の次のステップＳ３０６において、ＣＰＵ２０１は、外出予定に関するすべての設定項目についての設定入力が終

了したか否か判別し（ステップＳ３０６）、すべての設定入力が終了したと判別したときには、設定された項目情報を、通知連絡設定メモリ２２２に書き込み（ステップＳ３０７）、その後、テレビ受像機７の電源をオフして（ステップＳ３０８）、この設定処理ルーチンを終了する。

［通知連絡処理］

次に、以上のようにして帰宅予定または外出予定に関する通知設定がなされたときの、監視制御装置３における通知連絡の動作を、図３８～図４０を参照して説明する。

まず、監視制御装置３は、帰宅または外出に関する通知連絡の待機状態となっている（ステップＳ３１０）。この待機状態においては、セキュリティモードオン状態であってもよいし、また、セキュリティモードオフの状態であってもよい。

この待機状態において、ＣＰＵ２０１は、ドアロック制御装置１００からの情報を受信したか否か判別する（ステップＳ３１１）。そして、ドアロック制御装置１００からの情報を受信したと判別したときには、ＣＰＵ２０１は、受信した情報は、帰宅者情報であるか外出者情報であるかを判別する（ステップＳ３１２）。

ステップＳ３１２において、受信した情報は外出者情報であると判別したときには、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている外出予定者の識別情報と、ドアロック制御装置１００から受信した外出者情報に含まれる外出者の識別情報とを比較し、その比較結果に基づき、外出者は設定された外出予定者であるか否か判別し（ステップＳ３１３）、外出予定者でなければ、ステップＳ３１０に戻り、待機状態になる。

また、ステップＳ３１３において、外出者は設定された外出予定者であると判別したときには、ＣＰＵ２０１は、通知連絡設定メモリ２２２

に記憶されている外出通知連絡者の情報を読み出す。そして、この例においては、家族情報メモリ２０５に記憶されている外出通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該外出通知連絡者の例えば携帯電話端末に対して、設定された外出予定者が外出したことを電子メールにより通知連絡する（ステップＳ３１４）。この通知連絡には、外出した時刻の情報も含まれる。

そして、通知連絡をした後、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている当該外出予定に関する通知についての設定情報を消去して（ステップＳ３１５）、この処理ルーチンを終了する。

以上により、例えば、外出している親が、外出予定者として設定した子供が、予定の時刻に外出したかどうかを知ることができる。

ステップＳ３１２で、ドアロック制御装置１００から受信した情報が帰宅者情報であると判別したときには、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている帰宅予定者の識別情報と、ドアロック制御装置１００から受信した帰宅者情報に含まれる帰宅者の識別情報とを比較し、その比較結果に基づき、帰宅者は設定された帰宅予定者であるか否か判別し（ステップＳ３１６）、帰宅予定者でなければ、ステップＳ３１０に戻り、待機状態になる。

また、ステップＳ３１６において、帰宅者は設定された帰宅予定者であると判別したときには、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている帰宅通知連絡者の情報を読み出す。そして、この例においては、家族情報メモリ２０５に記憶されている外出通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該外出通知連絡者の例えば携帯電話端末に対して、当該帰宅通知連絡者に、設定された帰宅予定者が帰宅したことを電子メールにより通知連絡する（ステップＳ３１７）。この通知連絡には、帰宅した時刻の情報も含まれる。

そして、通知連絡をした後、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている当該帰宅予定に関する通知についての設定情報を消去して（ステップＳ３１５）、この処理ルーチンを終了する。

以上により、例えば、外出している親が、帰宅予定者として設定した子供が、予定の時刻に帰宅したかどうかを知ることができる。

次に、ステップＳ３１１において、ドアロック制御装置１００からの情報を受信してはいないと判別したときには、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている帰宅予定時刻と時計回路２２１が示す現在時刻とを比較し、帰宅予定時刻を経過したか否か判別する（ステップＳ３１８）。

ステップＳ３１８で、帰宅予定時刻は経過していないと判別したときには、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている外出予定時刻と時計回路２２１が示す現在時刻とを比較し、外出予定時刻を経過したか否か判別する（ステップＳ３１９）。ステップＳ３１９で、現在時刻が外出予定時刻も経過していないと判別したときには、ステップＳ３１０に戻り、待機状態になる。

ステップＳ３１８において、現在時刻が帰宅予定時刻を経過していると判別したときには、ＣＰＵ２０１は、帰宅予定者に帰宅を促す通知連絡を行なう（図３９のステップＳ３２１）。すなわち、家族情報メモリ２０５に記憶されている帰宅予定者のメールアドレスを読み出し、例えば、当該帰宅予定者の携帯電話端末に電子メールにより、速やかに帰宅すべき旨の通知を行なって、帰宅を促すようにする。

次に、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている帰宅通知連絡者の情報を読み出し、家族情報メモリ２０５に記憶されている当該帰宅通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該帰宅通知連絡者の例えば携帯電話端末に対して、設定さ

れた帰宅予定者が未だ帰宅していないことを電子メールにより通知連絡する（ステップＳ３２２）。

その後、ＣＰＵ２０１は、ドアロック制御装置１００からの帰宅者情報を待ち（ステップＳ３２３）、また、帰宅者情報を受信せずに所定時間、例えば１０分、経過したか否かを判別し（ステップＳ３２４）、所定時間経過していないと判別したときには、ステップＳ３２３に戻って、帰宅者情報の到来を待つ。また、ステップＳ３２４で所定時間経過したと判別したときには、ステップＳ３２１に戻り、再度、帰宅予定者に帰宅を促す電子メールを送る。

また、ステップＳ３２３でドアロック制御装置１００から帰宅者情報を受信したと判別したときには、ＣＰＵ２０１は、ドアロック制御装置１００からの帰宅者情報に含まれる識別信号により識別される帰宅者は、設定された帰宅予定者であるか否か判別する（ステップＳ３２５）。このステップＳ３２５で、帰宅者が設定された帰宅予定者でないと判別したときには、ＣＰＵ２０１は、ステップＳ３２４に進んで、所定時間の経過を待ち、ステップＳ３２４以降の上述の動作を繰り返す。

ステップＳ３２５で判別された帰宅者が予め設定された帰宅予定者であると判別したときには、ＣＰＵ２０１は、家族情報メモリ２０５に記憶されている帰宅通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該帰宅通知連絡者の例えば携帯電話端末に対して、当該帰宅通知連絡者に、設定された帰宅予定者が帰宅したことを電子メールにより通知連絡する（ステップＳ３１７）。この通知連絡には、帰宅した時刻の情報も含まれる。

そして、通知連絡をした後、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている当該帰宅予定者に関する設定情報を消去して（ステップＳ３１５）、この処理ルーチンを終了する。

また、ステップＳ３１９において、現在時刻が外出予定時刻を経過していると判別したときには、ＣＰＵ２０１は、外出予定者に外出を促す通知連絡を行なう（図４０のステップＳ３３１）。すなわち、家族情報メモリ２０５に記憶されている外出予定者のメールアドレスを読み出し、当該外出予定者の例えば携帯電話端末に、電子メールにより、速やかに外出すべき旨の通知を行なって、外出を促すようにする。これにより、外出予定者は、他事に忙殺されていたとしても、所定の外出予定時刻に外出することが可能となる。

次に、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている外出通知連絡者の情報を読み出し、家族情報メモリ２０５に記憶されている当該外出通知連絡者の個人情報を参照して、そのメールアドレスを読み出し、当該外出通知連絡者の例えば携帯電話端末に対して、設定された外出予定者が未だ外出していないことを電子メールにより通知連絡する（ステップＳ３３２）。

この通知連絡を受けた外出通知連絡者は、自宅に電話をかけるなどして、外出予定者に外出を促すことができる。外出予定者は、自分の携帯電話に電源が投入されていないなどの理由で、ステップＳ３３１で通知連絡を受けない場合においても、外部からの外出通知連絡者による電話連絡などにより促されて、外出予定時刻に外出することが可能になる。

その後、ＣＰＵ２０１は、ドアロック制御装置１００からの外出者情報を待ち（ステップＳ３３３）、また、外出者情報を受信せずに所定時間、例えば１０分、経過したか否かを判別し（ステップＳ３３４）、所定時間経過していないと判別したときには、ステップＳ３３３に戻って、外出者情報の到来を待つ。また、ステップＳ３３４で所定時間経過したと判別したときには、ステップＳ３３１に戻り、再度、外出予定者に外出を促す電子メールを送る。

また、ステップＳ３３３でドアロック制御装置１００から外出者情報を受信したと判別したときには、ＣＰＵ２０１は、外出者情報が含む識別信号により識別される外出者は、設定された外出予定者であるか否か判別する（ステップＳ３３５）。このステップＳ３３５で、外出者が設定された外出予定者でないと判別したときには、ＣＰＵ２０１は、ステップＳ３３４に進んで、所定時間の経過を待ち、ステップＳ３３４以降の上述の動作を繰り返す。

ステップＳ３３５で判別された外出者が予め設定された外出予定者であると判別したときには、ＣＰＵ２０１は、家族情報メモリ２０５に記憶されている外出通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該外出通知連絡者の例えば携帯電話端末に対して、当該外出通知連絡者に、設定された外出予定者が外出したことを電子メールにより通知連絡する（ステップＳ３１４）。この通知連絡には、外出した時刻の情報も含まれる。

そして、通知連絡をした後、ＣＰＵ２０１は、通知連絡設定メモリ２２２に記憶されている当該外出予定者に関する設定情報を消去して（ステップＳ３１５）、この処理ルーチンを終了する。

以上のようにして、この実施形態によれば、例えば親が、子供を帰宅予定者として設定すると共に、帰宅予定時刻を設定し、さらに、当該親を帰宅通知連絡者に設定しておくことにより、親は、子供が予定された帰宅時刻に帰宅しているかどうかを確認することができると共に、子供に速やかな帰宅を促すことができる。

また、外出を予定している者が、外出予定時刻を設定しておくことにより、外出予定時刻を失念してしまっても、外出予定時刻になると外出を促すようにされるので、確実に予定した時刻に外出することが可能になる。

［他の実施形態］

上述の実施形態では、所定の予約設定時刻になったときに、帰宅予定者や外出予定者、および予め設定した帰宅通知連絡者、外出通知連絡者に、帰宅予定者や外出予定者の帰宅状況、外出状況を通知連絡するようにしたが、ドアロック制御装置１００と、電子鍵装置との通信を行なって、外出あるいは帰宅する者についての情報を、予め設定した通知連絡者に通知連絡するようにしても勿論よい。

また、以上の実施形態では、通信装置は、ドアロック装置２とセキュリティシステムの監視制御装置３とを含む構成としたが、ドアの施錠および開錠のみを目的とするドアロック制御システムとして考えた場合には、監視制御装置３は不要であって、通信装置は、ドアロック装置２のみで構成することもできる。その場合には、ドアロック装置２は、電話回線を通じて携帯電話端末にメールや電話をかける機能を備えるものである。

また、通知連絡の方法は、電子メールとしたが、音声合成などを用いることにより、電話を携帯電話端末や予め定められた電話番号の固定電話端末にかけて、音声情報として、帰宅や外出を促す通知や、帰宅状況や外出状況を通知するようにすることもできる。

また、上述の実施形態では、電子鍵情報をＩＣチップの製造番号とし、これと個人情報とを対応させることにより、電子鍵情報を個人識別情報としても用いるようにしたが、電子鍵情報と共に、予め個人識別情報を定めて電子鍵装置や、ドアロック制御装置、監視制御装置などに登録しておき、電子鍵装置と、リード／ライト部との通信の際に電子鍵情報と共に、個人識別情報をやり取りするようにしてもよい。その場合には、電子鍵情報のほかに、各個人ごとに識別情報が設定され、それが電子鍵装置のメモリに記憶されると共に、ドアロック制御装置や監視制御装置

のメモリの個人プロファイル情報に含められて記憶される。

そのように個人識別情報を電子鍵情報と別個とする場合には、一つのドアロック装置に一つの電子鍵情報として、当該家に住む家族構成員の全員に共通の一つの電子鍵情報を用いるようにして、各人が、その共通鍵情報を格納する電子鍵装置をそれぞれ持つようにすることもできる。

また、上述の実施形態では、通知連絡者への連絡のための情報、例えば電子メールアドレスや、電話番号あるいはパーソナルコンピュータに通知する場合にはＩＰアドレスは、監視制御装置やドアロック制御装置に予め記憶されている情報を読み出して用いるようにしたが、電子鍵装置との通信時に電子鍵装置から取得するように構成してもよい。

上述の実施形態は、セキュリティ監視システムも含む通信システムの構成であったので、管理サーバ装置１０が存在しているが、セキュリティ監視システムが存在しない通信システムの構成も可能である。

なお、電子鍵情報は、管理サーバ装置からドアロック装置の電子鍵情報の記憶部に転送して、登録するのではなく、住戸に設置する前に、予め、ドアロック装置に登録して記憶しておくようにしても勿論よい。特に、上述の実施形態のようなセキュリティ監視システムを用いずに、ドアロック制御システムを単独で使用するような場合には、そのようにするものである。

また、ＩＣチップのメモリには、予め一元管理された識別情報が記憶されているように説明したが、後から、一元管理されている識別情報が書き込まれるようにされてもよいことは言うまでもない。

なお、上述の実施形態では、電子鍵装置を、外側電子鍵リード／ライト部２１ｅｘに対して、ドアの施錠後、所定時間以内にかざした場合に、セキュリティモードをオンにするようにしたが、ドアロック制御装置１００または監視制御装置３では、玄関ドア１からの入退出を管理してい

るので、在宅者が無くなったら、自動的にセキュリティレベルＡでセキュリティモードをオンにするようにすることもできる。

その場合に、ドアロック制御装置１００で、在宅者無しを検出したときに、監視制御装置３にセキュリティモードオンを要求しても良いし、監視制御装置３が、自装置で、在宅者無しを検出したときに、セキュリティモードオンとするようにしても良い。

なお、この例では、在宅者が玄関ドア１を開錠し、玄関ドア１を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしたが、セキュリティモードがオンになっているときに外出者があった場合には、外出者を電子鍵装置との通信により取得される識別情報により認識して、監視制御装置３が、帰宅者があった場合と全く同様にして、在宅状況の変化に対応して自動的にセキュリティレベルを変更するようにすることもできる。

なお、以上の実施形態の説明では、鍵情報としての識別情報の認証は、ドアロック装置で行なうようにしたが、ドアロック装置２は、監視制御装置３に、あるいは監視制御装置３を介して管理サーバ装置１０に鍵情報を送り、監視制御装置３あるいは管理サーバ装置１０で、認証作業を行ない、その認証結果を、ドアロック装置２に返す（管理サーバ装置１０の場合には監視制御装置３を介して返す）ようにしても良い。その場合には、監視制御装置３からドアロック制御装置１００への鍵情報の転送や抹消指示を送る必要はない。

また、開錠者、施錠者の識別情報も監視制御装置３ではなく、管理サーバ装置１０に送り、管理サーバ装置１０により、セキュリティ管理をするようにしてもよい。

また、以上の説明では、外出者か帰宅者かは、ドアロック制御装置１００で判別するようにしたが、監視制御装置３においても、ドアロック

制御装置１００でのドアロック制御モードの設定情報を備えているので、ドアロック制御装置１００は、ＩＣカード４０Ｆが、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘにかざされて通信が両者の間で行なわれ、識別情報についての認証がとれたときには、その識別情報と、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのいずれと通信したかの情報と、開錠か施錠かの情報とを、監視制御装置３に送り、監視制御装置３が、外出か帰宅かを判別するようにすることもできる。

なお、電子鍵装置は、上述もしたように、ＩＣカードに限られるものではなく、上述の例の場合であれば、ＩＣカードと同様のＩＣチップや、通信手段および生体情報の取得手段などを備える携帯電話端末やＰＤＡ（携帯情報端末）などを用いることができるものである。

また、電子鍵装置は、上述の実施形態のような非接触形式で電子鍵情報の通信を行なうのものに限られるものではなく、接触形式で電子鍵情報の通信を行なうものであっても勿論よい。

産業上の利用可能性

以上説明したように、この発明による通信装置によれば、ドアの施錠、開錠を行なう個人を管理することにより、帰宅予定者や外出予定者に帰宅や外出を促すことができると共に、帰宅状況や外出状況を、外出中の通知連絡者に通知連絡することが可能になる。

請　求　の　範　囲

1．　少なくとも電子鍵情報を記憶する電子鍵装置と通信を行なう第１の通信手段と、

通信ネットワークを通じて情報送信を行なうための第２の通信手段と、

電子鍵情報を記憶する記憶部と、

前記第１の通信手段を通じて前記電子鍵装置から受信する電子鍵情報と、前記記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいてドアのロック機構を制御するドアロック制御手段と、

前記第１の通信手段を通じて前記電子鍵装置から受信した情報に基づいて当該電子鍵装置の使用者を認識する使用者認識手段と、

前記使用者認識手段での認識結果に基づいて、前記電子鍵装置の使用者の入退出に関する情報を、予め定められている通知先に前記第２の通信手段を介して送信するように制御する送信制御手段と、

を備えることを特徴とする通信装置。

2．　請求項１に記載の通信装置において、

前記通知先に入退出に関する情報を送信すべき前記電子鍵装置の使用者の設定を受け付けて記憶する設定記憶手段を備え、

前記送信制御手段は、前記設定された前記電子鍵装置の使用者の入退出に関する情報を、前記第２の通信手段を介して前記通知先に送信することを特徴とする通信装置。

3．　請求項２に記載の通信装置において、

前記設定記憶手段では、前記電子鍵装置の使用者と共に、当該使用者に対応して時刻情報の設定入力を受け付けて記憶し、

前記送信制御手段は、前記設定入力された時刻情報に対応する時刻を経過しても、前記使用者認識手段で前記設定された前記電子鍵装置の使

用者を認識しなかったときに、当該電子鍵装置の使用者の入退出がなされていないことに関する情報を、前記通知先に前記第２の通信手段を介して送信するように制御する

ことを特徴とする通信装置。

４．　請求項３に記載の通信装置において、

前記通知先は、前記設定された前記電子鍵装置の使用者であり、前記電子鍵装置の使用者の入退出がなされていないことに関する情報は、前記入退出を促す情報である

ことを特徴とする通信装置。

５．　請求項３に記載の通信装置において、

前記通知先は、前記設定された前記電子鍵装置の使用者以外である

ことを特徴とする通信装置。

６．　請求項５に記載の通信装置において、

前記設定された時刻情報に対応する時刻の経過後に、前記使用者認識手段で前記設定された前記電子鍵装置の使用者を認識したときに、当該電子鍵装置の使用者の入退出に関する情報を、前記通知先に前記第２の通信手段を介して送信するように制御する

ことを特徴とする通信装置。

７．　請求項１に記載の通信装置において、

前記電子鍵情報は、前記電子鍵装置の使用者を識別することが可能な識別情報で構成され、

前記使用者認識手段は、前記電子鍵装置から受信した前記電子鍵情報に基づいて前記ドアから入退出した前記電子鍵装置の使用者を認識する

ことを特徴とする通信装置。

８．　請求項１に記載の通信装置において、

前記電子鍵情報は、同一のものが存在しないように一元管理されて割

り振られた識別情報であり、

前記電子鍵情報に対応して前記電子鍵装置の所有者を特定可能とする個人情報を記憶する個人情報記憶部を備えるとともに、前記電子鍵装置から受信した前記電子鍵情報と、前記記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいて、前記電子鍵装置の所有者の前記ドアからの入退出を管理する手段を備えると共に、

前記使用者認識手段は、前記電子鍵装置から受信した前記電子鍵情報に基づいて前記ドアから入退出した前記電子鍵装置の使用者を認識することを特徴とする通信装置。

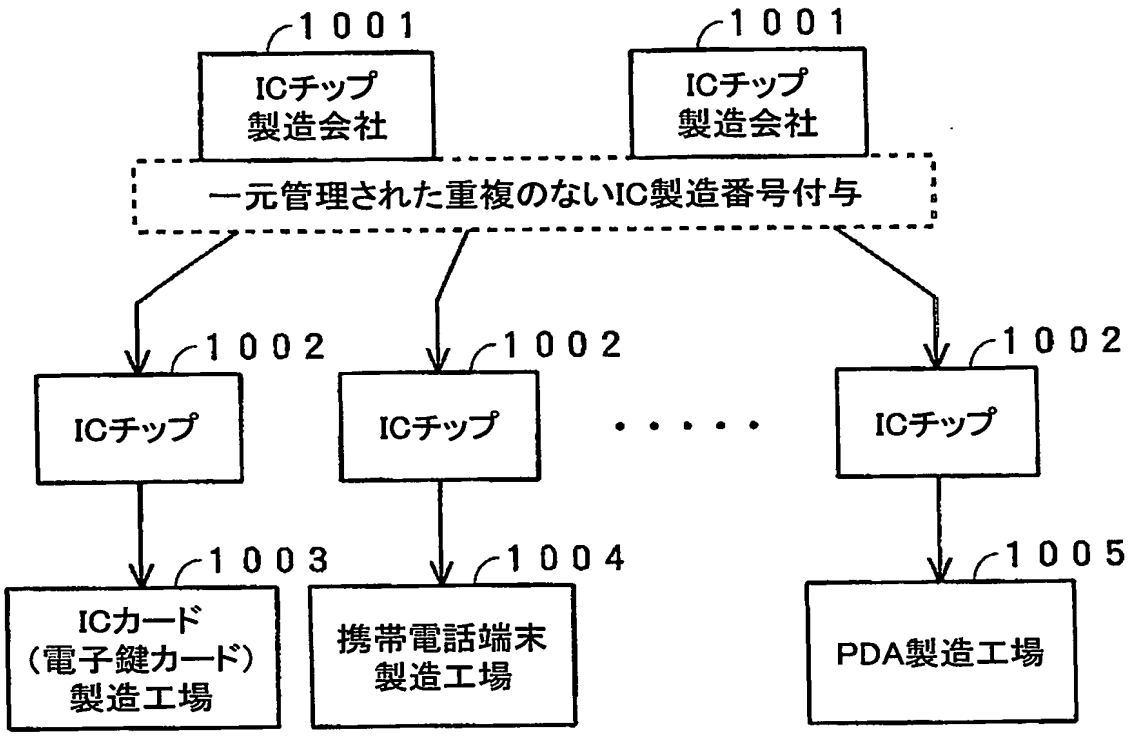

1001
ICチップ
製造会社
1001
ICチップ
製造会社
一元管理された重複のないIC製造番号付与
1002
ICチップ
1002
ICチップ
1002
ICチップ
1003
ICカード
(電子鍵カード)
製造工場
1004
携帯電話端末
製造工場
1005
PDA製造工場

Fig.1


00AKKK0001
メーカー番号
カテゴリコード
シリアル番号

Fig.2

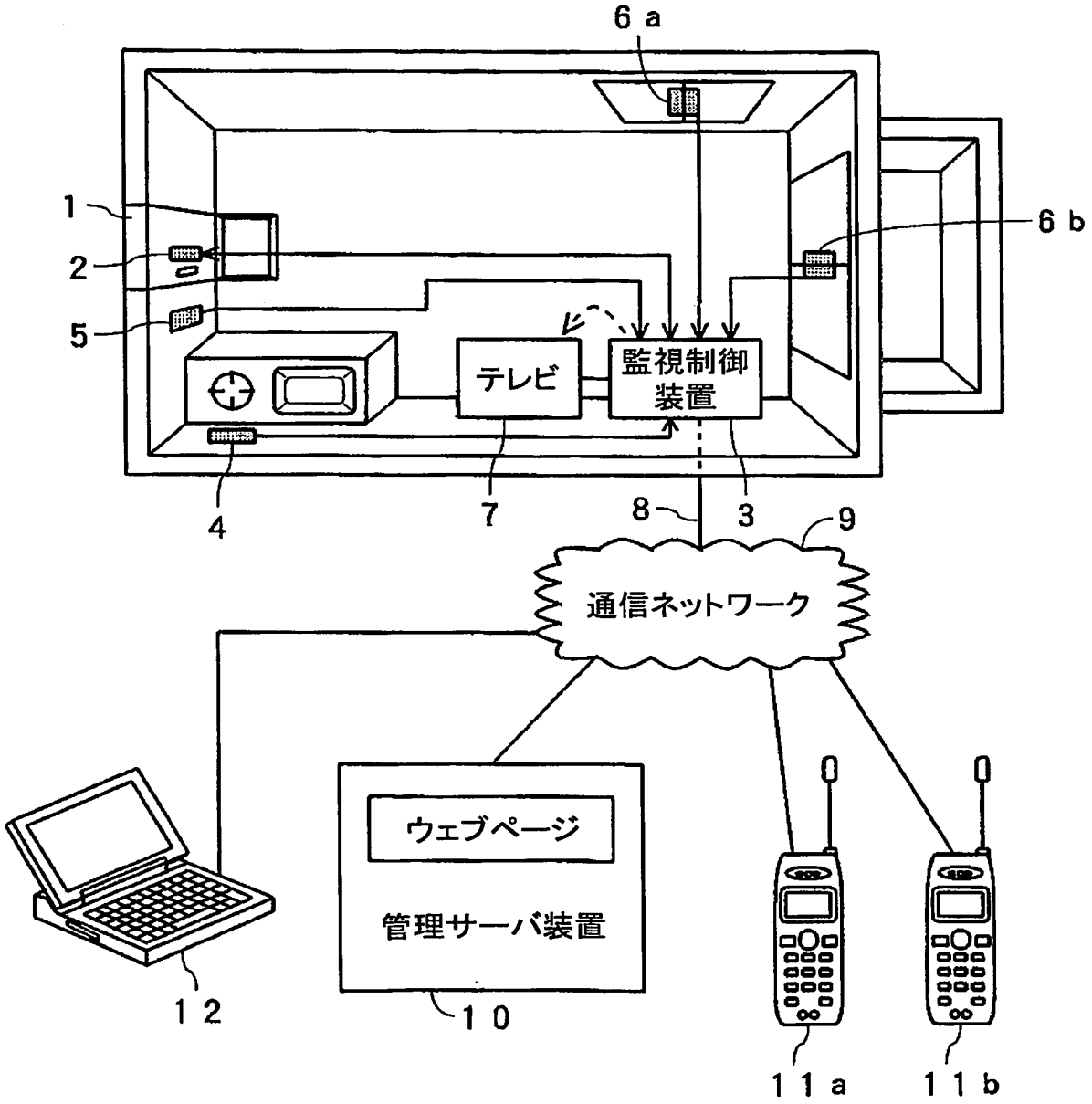

6 a
1
2
5
6 b
テレビ
監視制御
装置
4
7
8
3
9
通信ネットワーク
ウェブページ
管理サーバ装置
1 2
1 0
1 1 a
1 1 b

Fig.3

Fig.4A

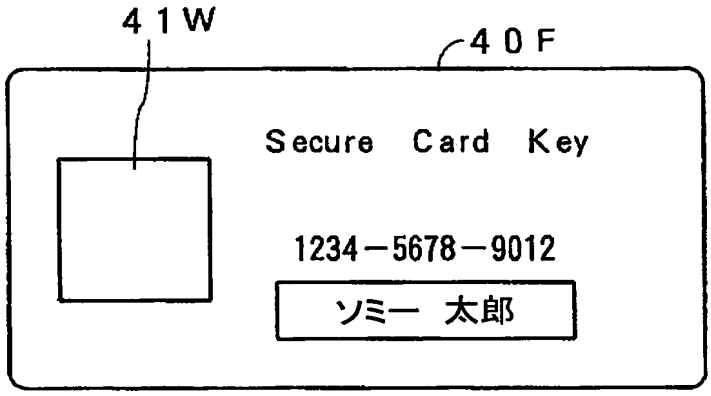
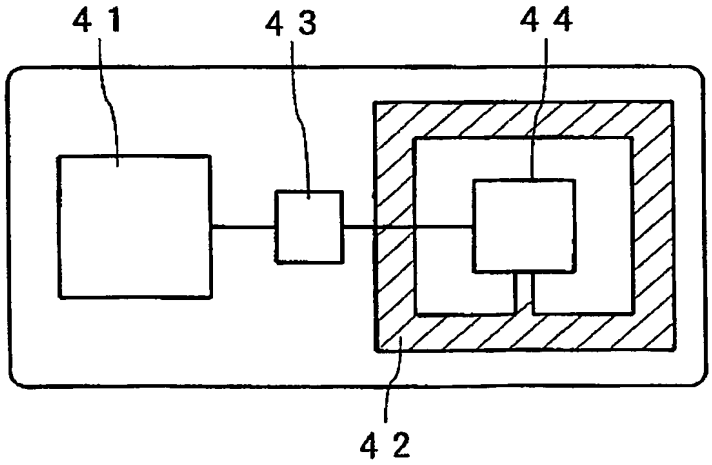


Fig.4B



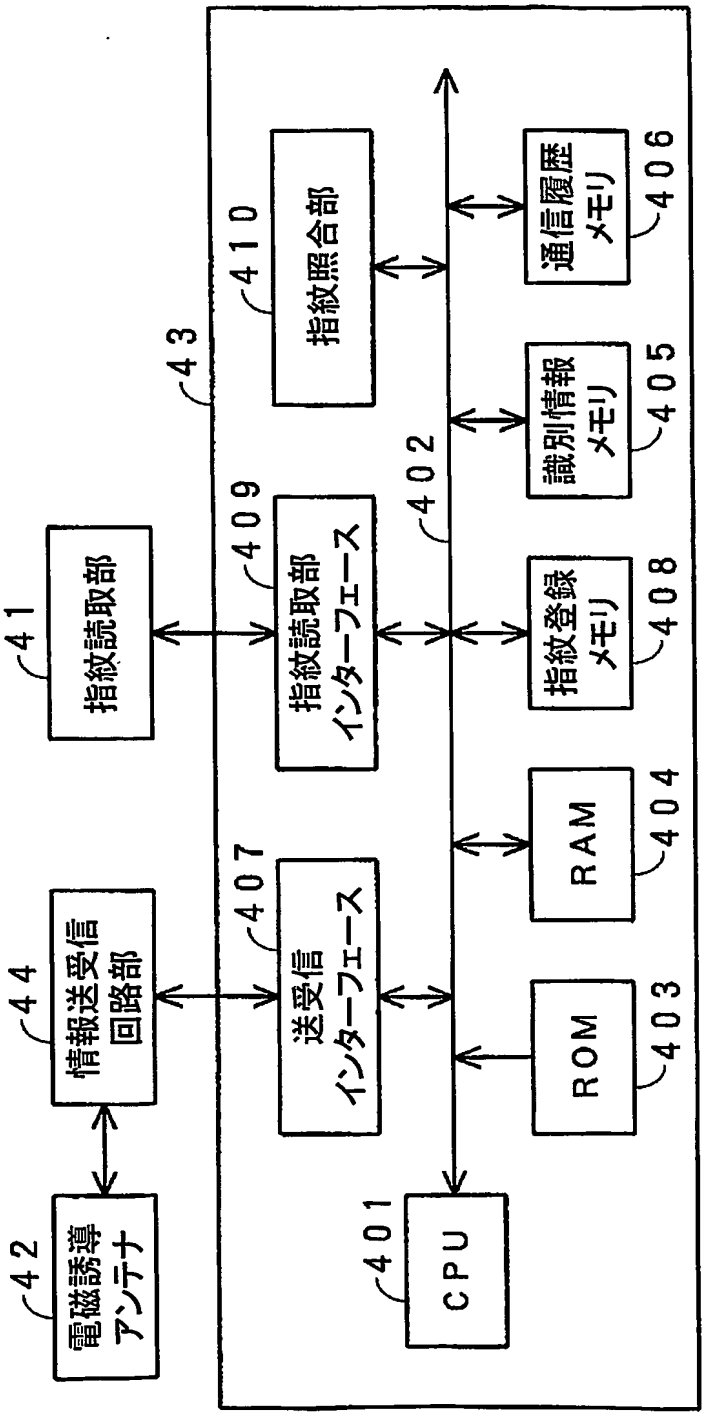

42
電磁誘導
アンテナ
44
情報送受信
回路部
41
指紋読取部
43
401
CPU
403
ROM
404
RAM
407
送受信
インターフェース
409
指紋読取部
インターフェース
402
410
指紋照合部
408
指紋登録
メモリ
405
識別情報
メモリ
406
通信履歴
メモリ

Fig.5

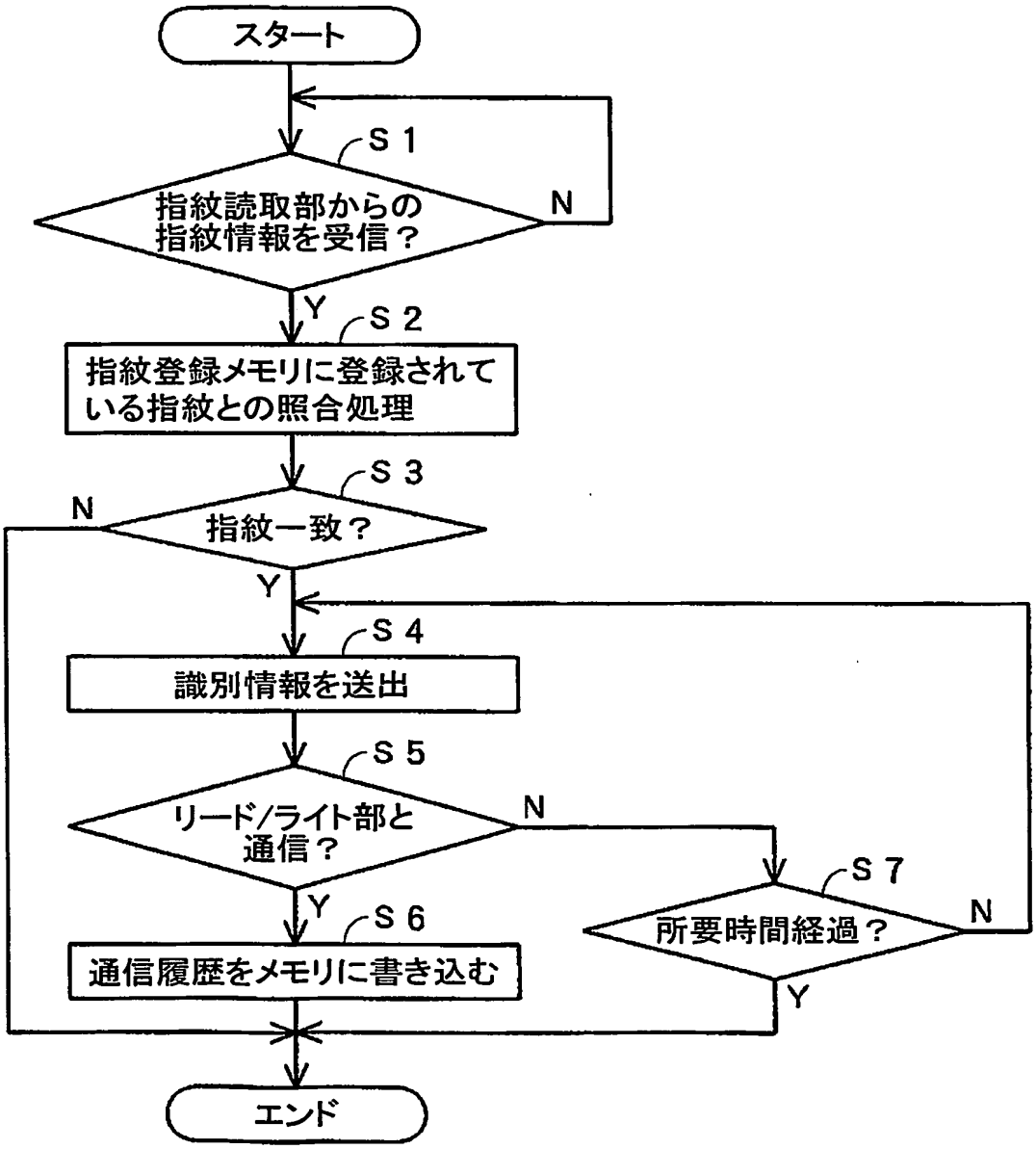

スタート
S 1
指紋読取部からの
指紋情報を受信？
N
Y
S 2
指紋登録メモリに登録されて
いる指紋との照合処理
S 3
N
指紋一致？
Y
S 4
識別情報を送出
S 5
リード/ライト部と
通信？
N
Y
S 6
通信履歴をメモリに書き込む
S 7
所要時間経過？
N
Y
エンド

Fig.6

Fig.7A

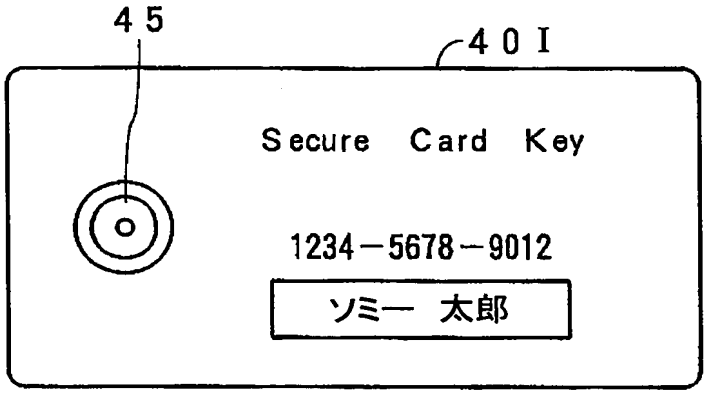
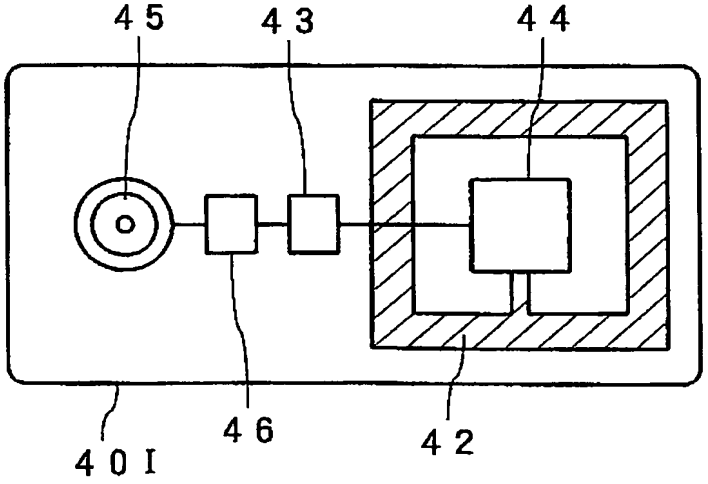


Fig.7B



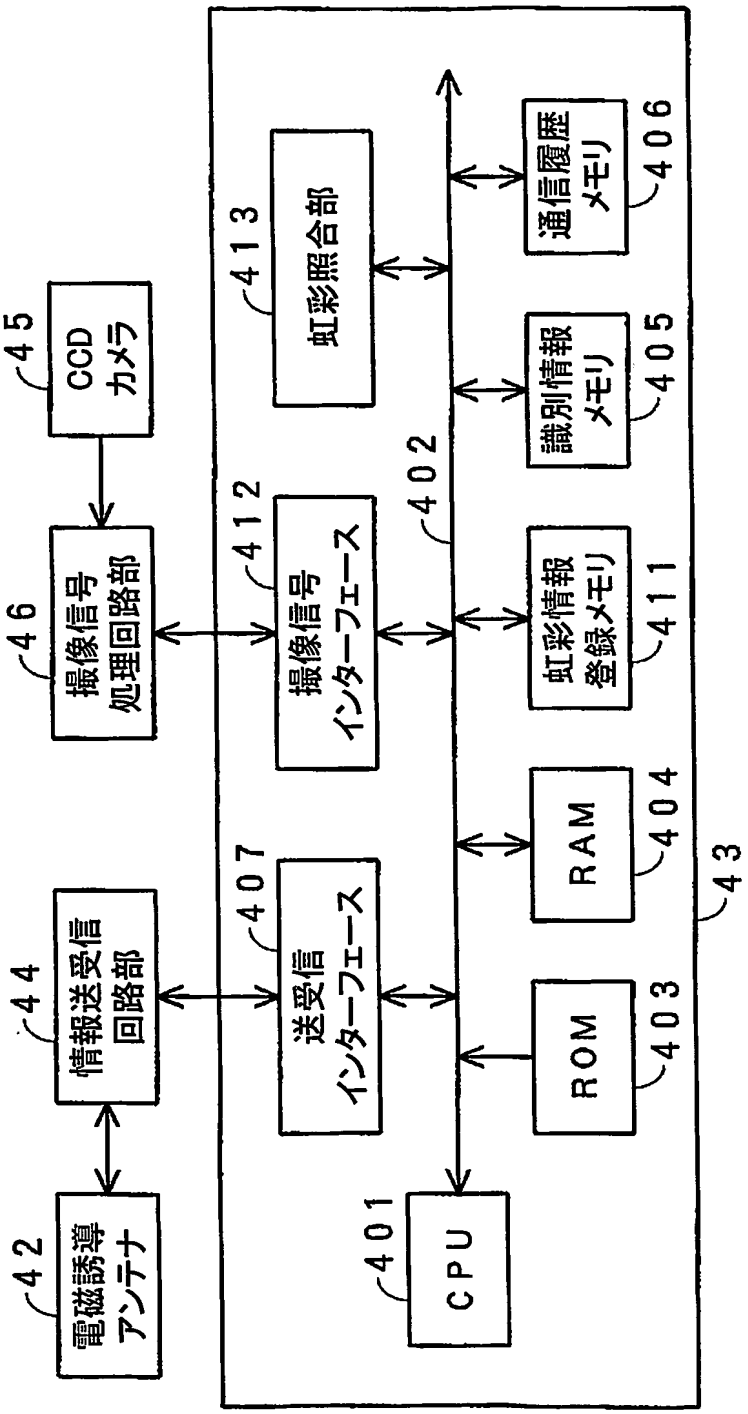

電磁誘導アンテナ
42
情報送受信回路部
44
撮像信号処理回路部
46
CCD カメラ
45
送受信インターフェース
407
撮像信号インターフェース
412
虹彩照合部
413
CPU
401
ROM
403
RAM
404
虹彩情報登録メモリ
411
識別情報メモリ
405
通信履歴メモリ
406
402
43

Fig.8

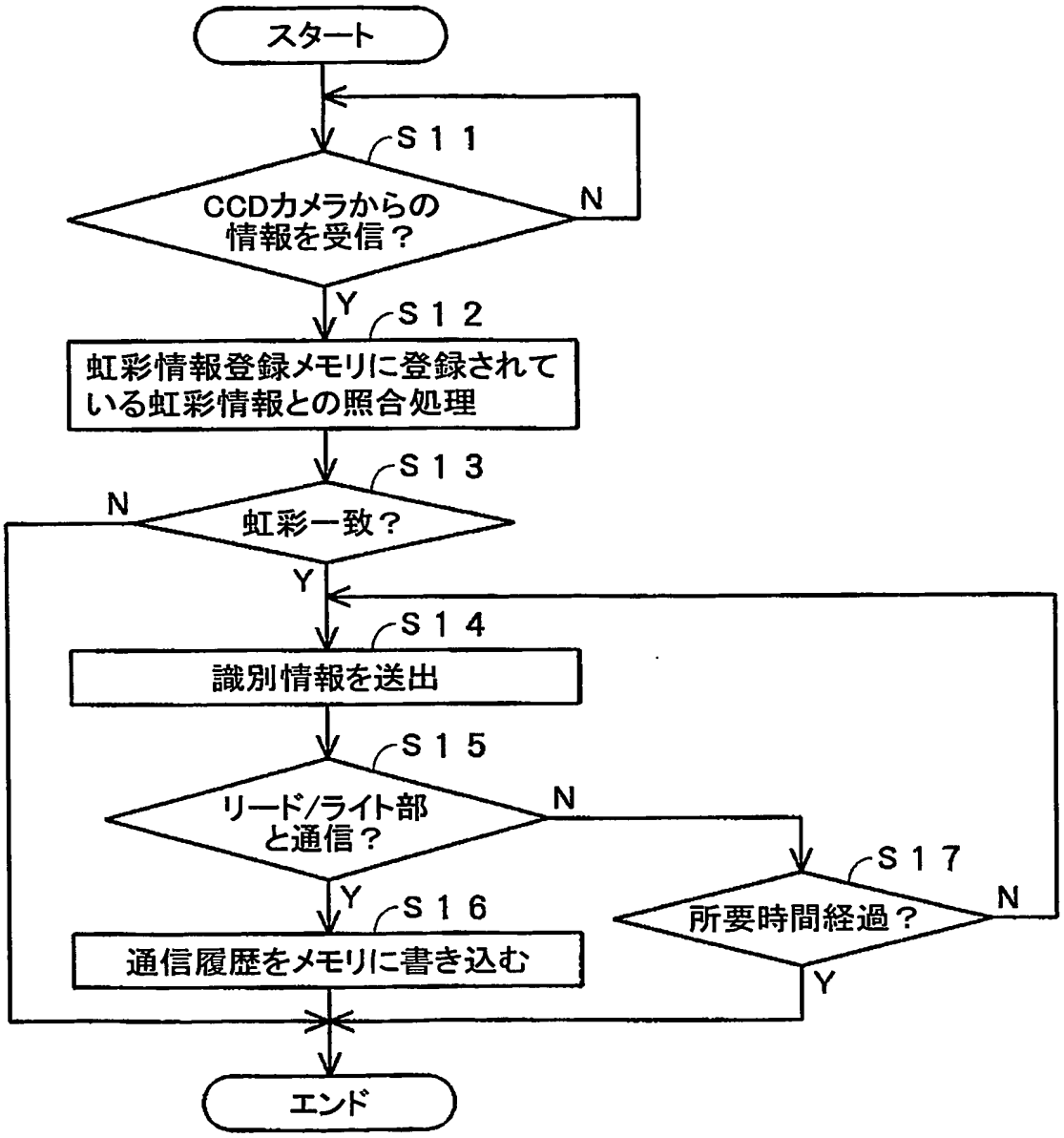

スタート
S11
CCDカメラからの情報を受信？
N
Y
S12
虹彩情報登録メモリに登録されている虹彩情報との照合処理
S13
虹彩一致？
N
Y
S14
識別情報を送出
S15
リード/ライト部と通信？
N
Y
S16
通信履歴をメモリに書き込む
S17
所要時間経過？
N
Y
エンド

Fig.9

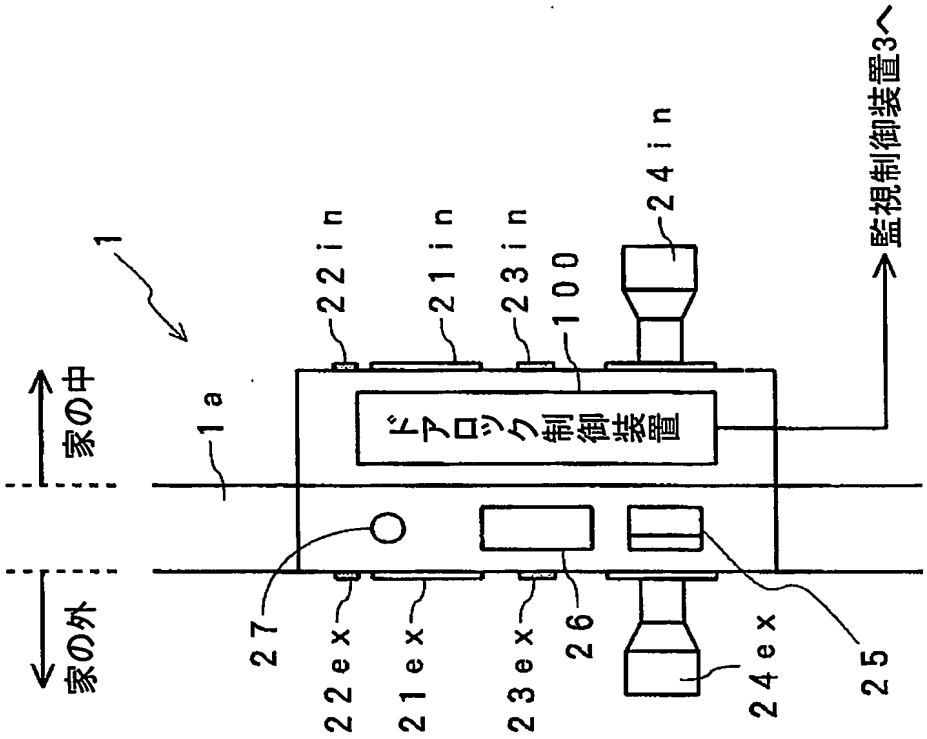


Fig.10B

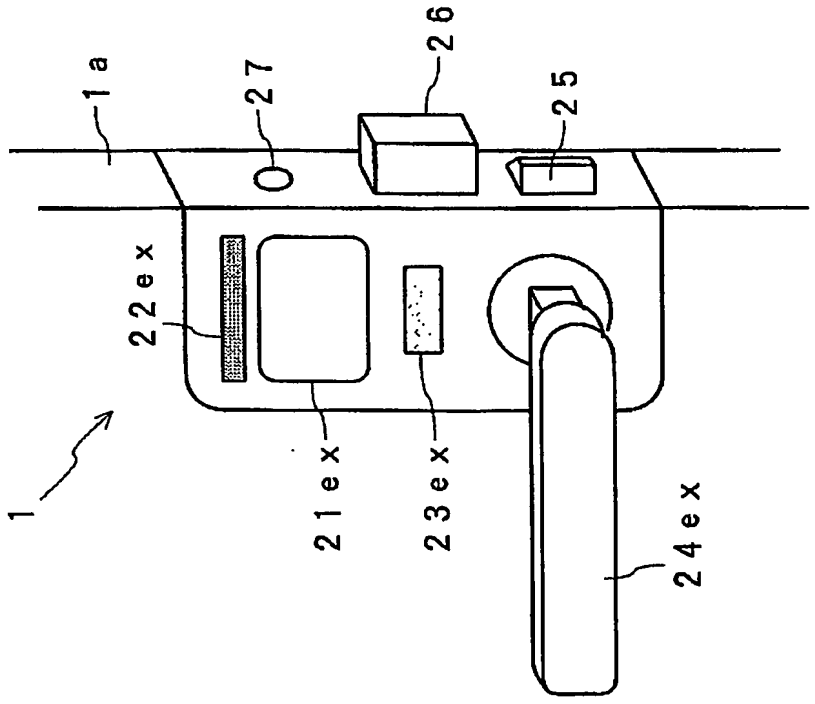


Fig.10A

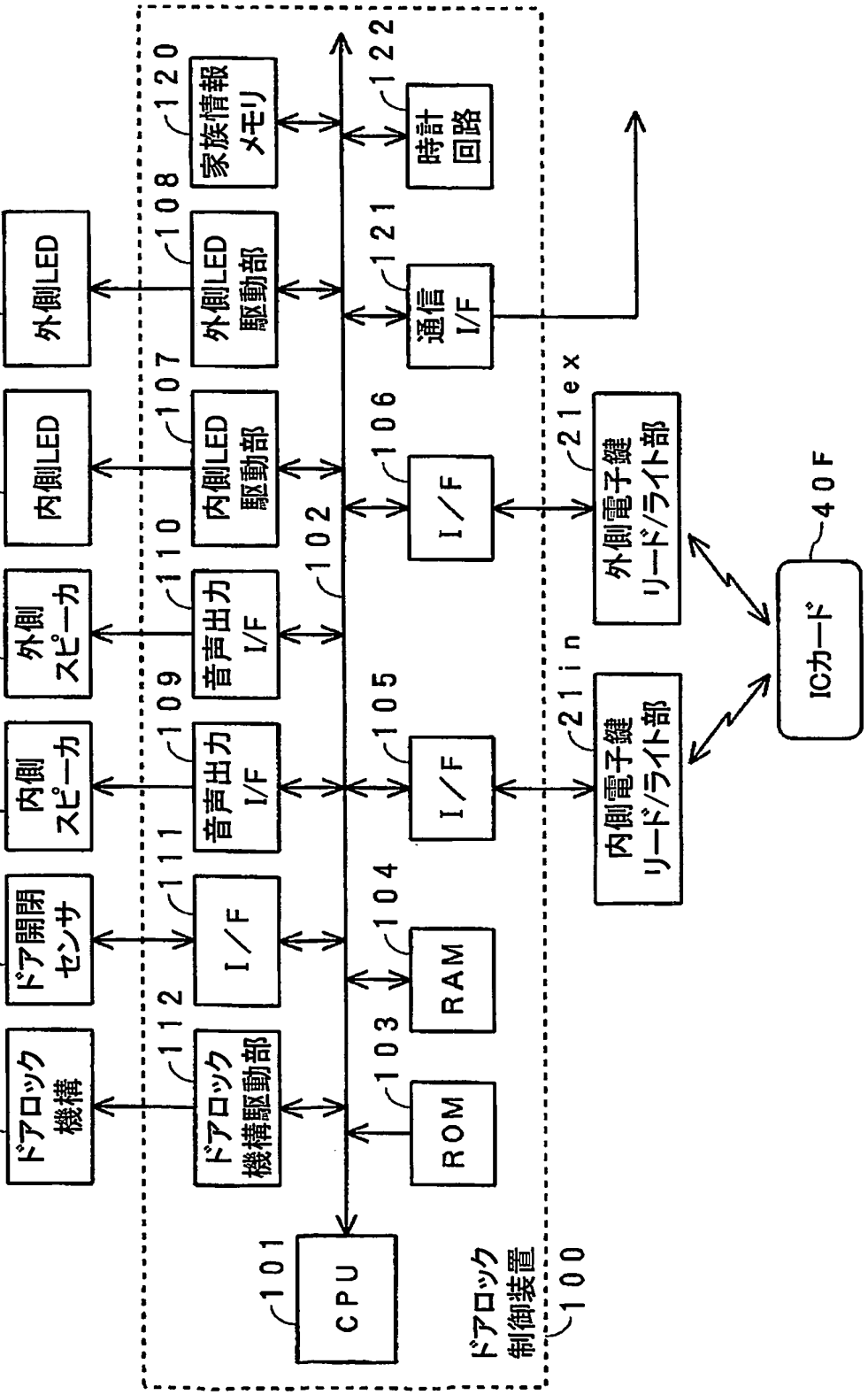

2
ドアロック制御装置 100
CPU 101
ROM 103
RAM 104
I／F 105
I／F 106
I／F 111
I／F 112
音声出力 I/F 109
音声出力 I/F 110
内側LED 駆動部 107
外側LED 駆動部 108
家族情報 メモリ 120
時計 回路 122
通信 I/F 121
ドアロック 機構駆動部
内側 スピーカ 23in
外側 スピーカ 23ex
内側LED 22in
外側LED 22ex
ドア開閉 センサ 27
ドアロック 機構 28
内側電子鍵 リード/ライト部 21in
外側電子鍵 リード/ライト部 21ex
ICカード 40F

Fig.11

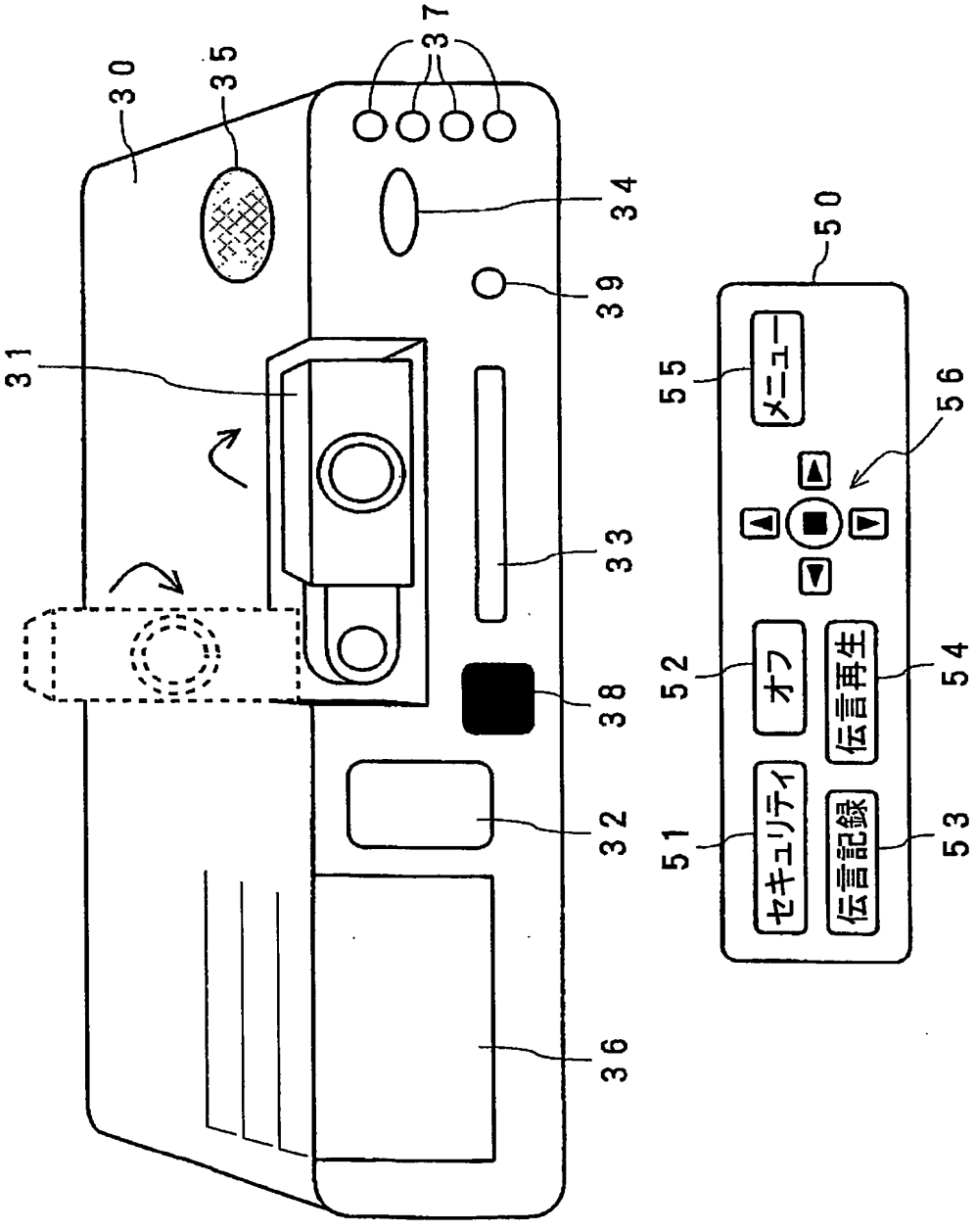

3
30
35
37
34
39
31
33
38
32
36
50
55
メニュー
56
52
オフ
54
伝言再生
51
セキュリティ
53
伝言記録

Fig.12

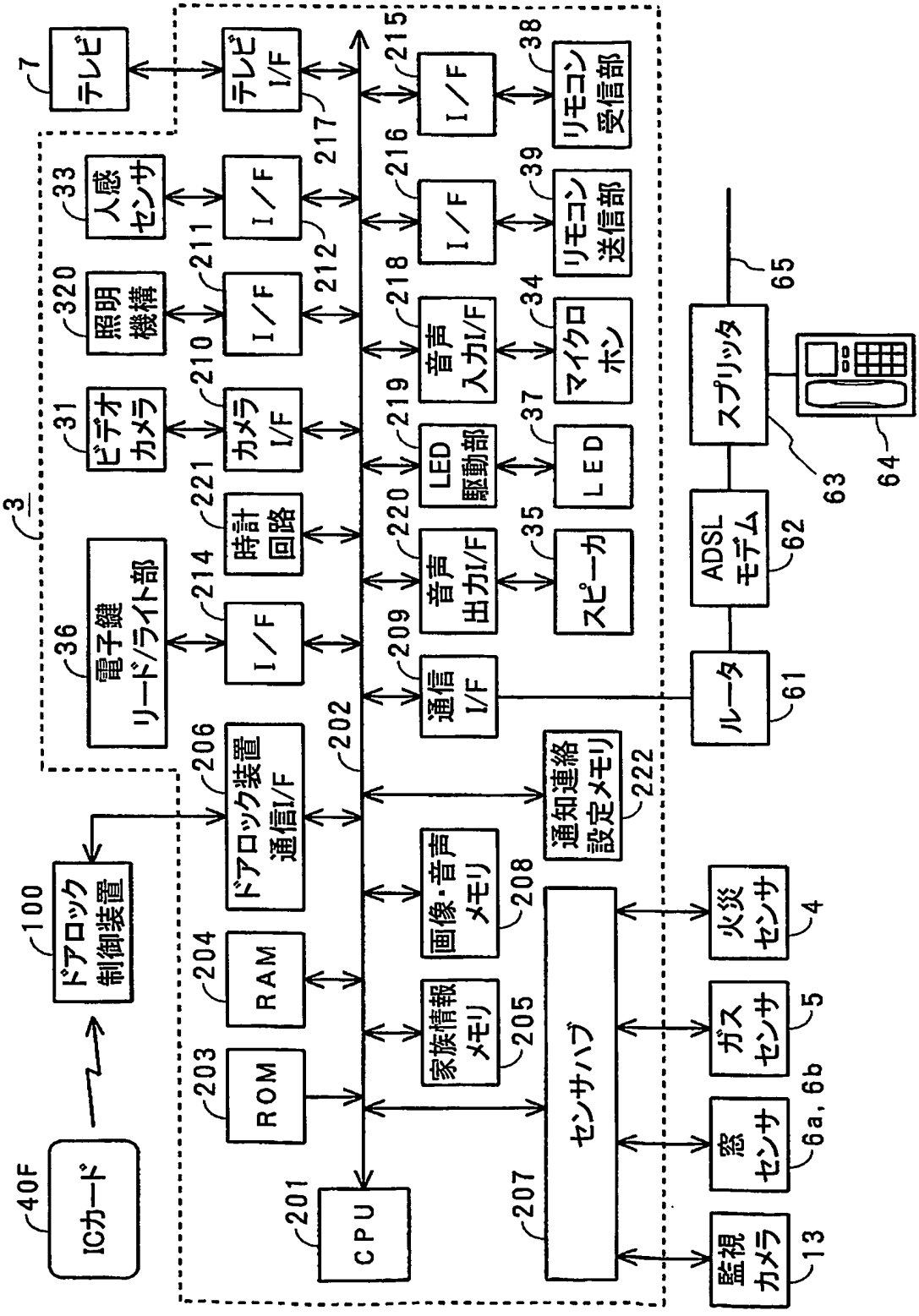

7
テレビ
テレビ I/F
215
I／F
38
リモコン 受信部
33
人感センサ
211
I／F
216
I／F
39
リモコン 送信部
320
照明機構
210
I／F
212
218
音声入力I/F
34
マイクロホン
31
ビデオカメラ
カメラ I/F
221
219
LED 駆動部
37
LED
3
時計回路
214
220
音声出力I/F
35
スピーカ
36
電子鍵 リードライト部
I／F
209
通信 I/F
ルータ
61
ADSL モデム
62
スプリッタ
65
63
64
206
ドアロック装置 通信I/F
202
222
通知連絡設定メモリ
100
ドアロック制御装置
208
画像・音声メモリ
204
RAM
205
家族情報メモリ
203
ROM
207
センサハブ
201
CPU
40F
ICカード
4
火災センサ
5
ガスセンサ
6a, 6b
窓センサ
13
監視カメラ

Fig.13

	識別情報(ICチップ製造番号) ・本鍵情報 ・バックアップ鍵情報	個人識別情報
	パスワード	個人情報
	氏名	
	住所	
	生年月日	
	年齢	
	続柄	
	登録日	
	銀行口座番号	
	電話番号	
	電子メールアドレス	
	IPアドレス	
	趣味/嗜好情報 ・好きなテレビ番組:ドラマ ・好きな音楽:ジャズ ・好きな映画:SF	
	入退出履歴情報	
	電子鍵登録・紛失履歴情報	

Fig.14

セキュリティレベル	父親	母親	子供
D	○	○	○
D	○	○	×
D	○	×	○
D	○	×	×
C	×	○	○
C	×	○	×
B	×	×	○
A	×	×	×

○：在宅
×：不在

Fig.15

セキュリティレベル	窓・ドア監視	火災・ガス監視	カメラ監視
A	○	○	○
B	○	○	×
C	×	○	×
D	×	×	×

Fig.16

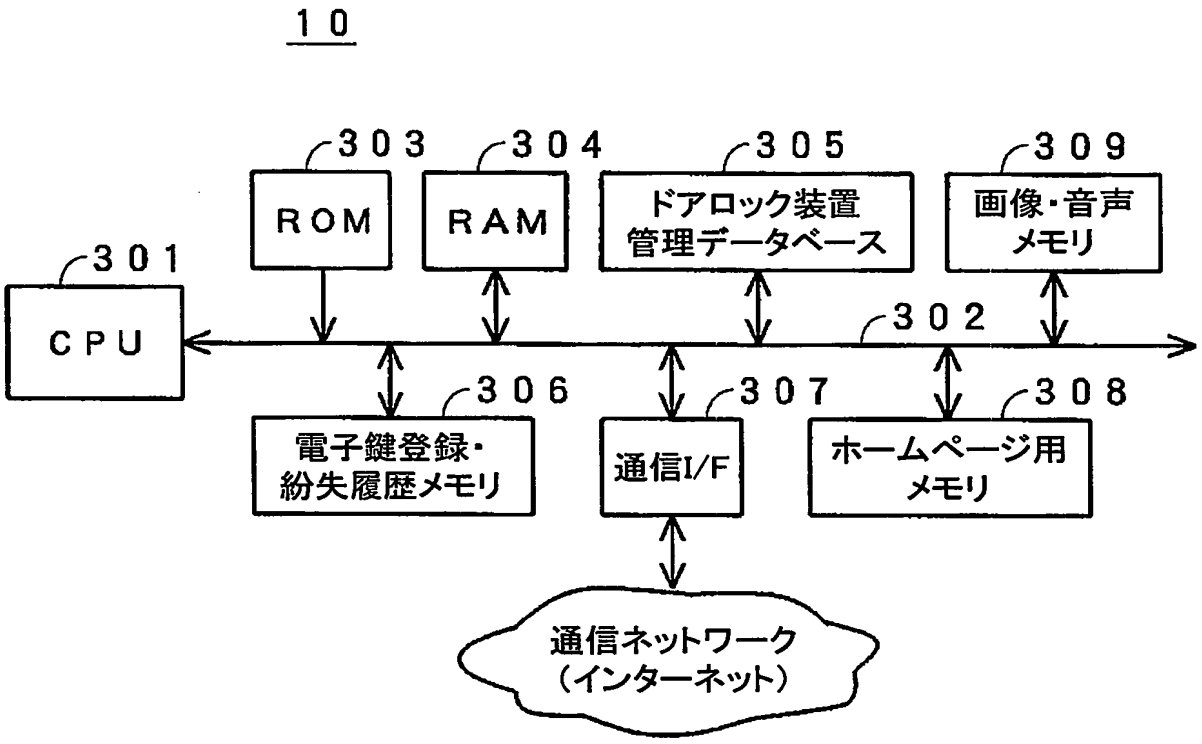

10
303
304
305
309
ROM
RAM
ドアロック装置
管理データベース
画像・音声
メモリ
301
CPU
302
306
307
308
電子鍵登録・
紛失履歴メモリ
通信I/F
ホームページ用
メモリ
通信ネットワーク
（インターネット）

Fig.17

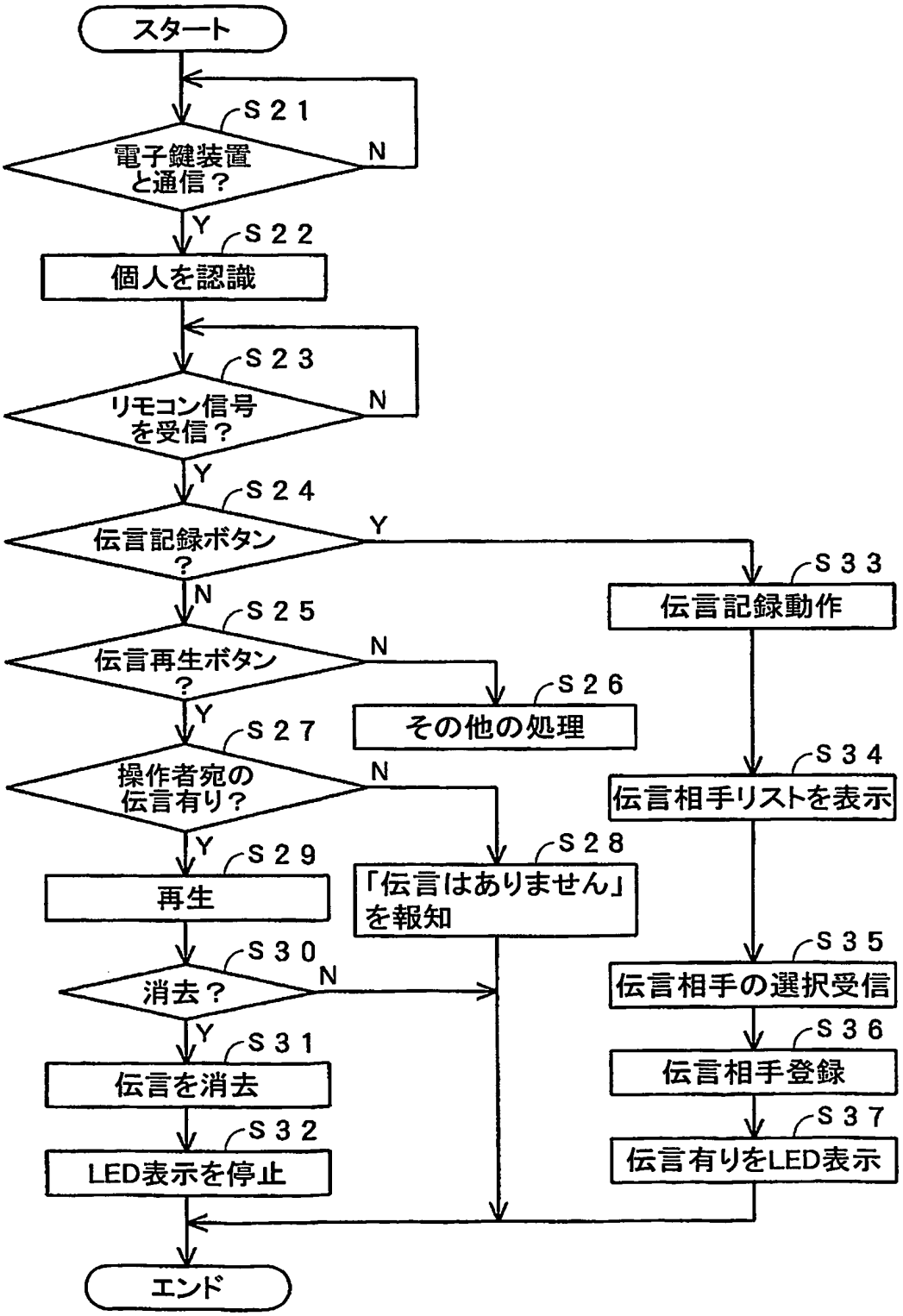

スタート
S21
電子鍵装置と通信？
N
Y
S22
個人を認識
S23
リモコン信号を受信？
N
Y
S24
伝言記録ボタン？
Y
N
S25
伝言再生ボタン？
N
Y
S26
その他の処理
S27
操作者宛の伝言有り？
N
Y
S28
「伝言はありません」を報知
S29
再生
S30
消去？
N
Y
S31
伝言を消去
S32
LED表示を停止
エンド
S33
伝言記録動作
S34
伝言相手リストを表示
S35
伝言相手の選択受信
S36
伝言相手登録
S37
伝言有りをLED表示

Fig.18

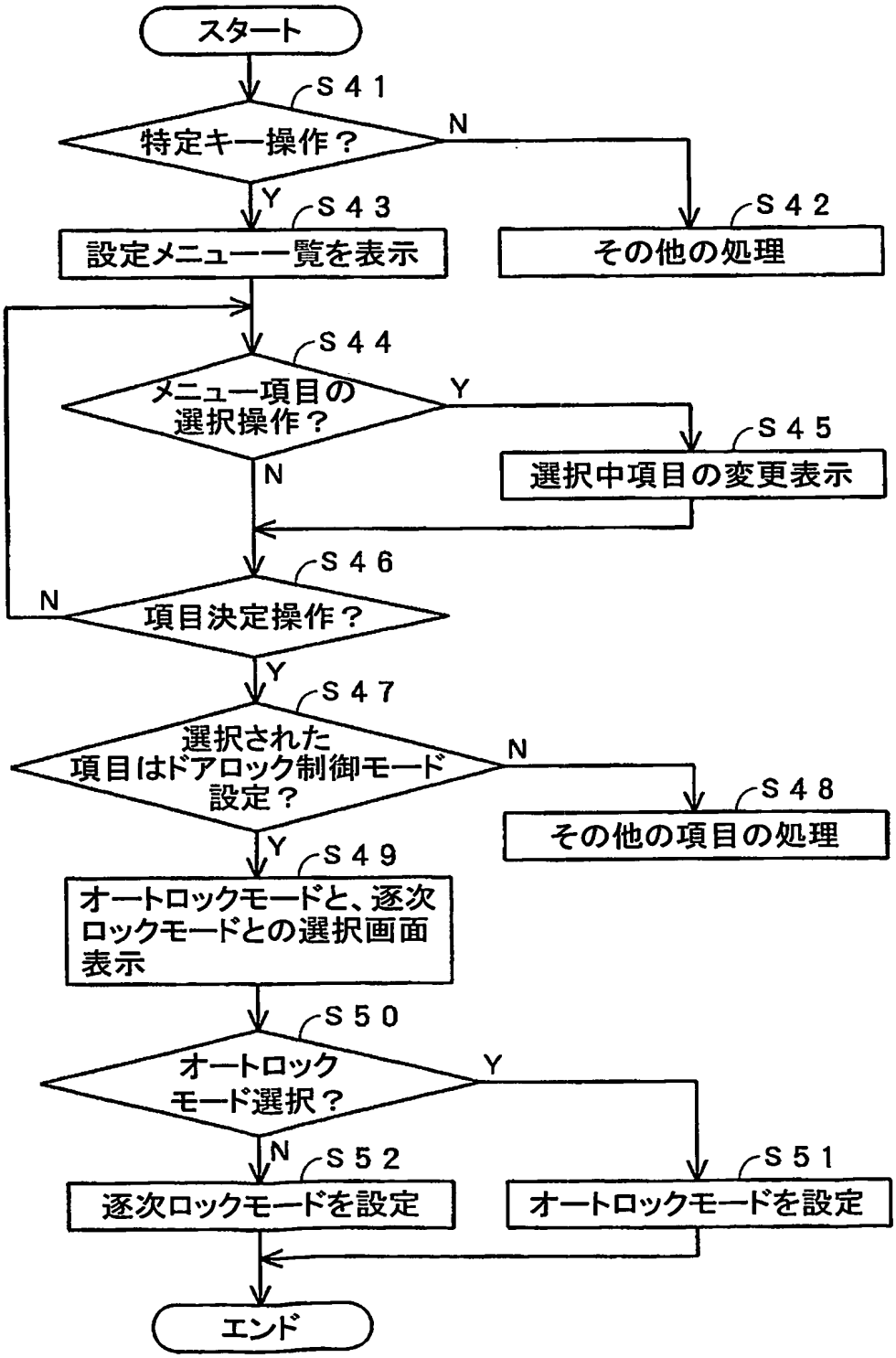

スタート
S41
特定キー操作？
N
Y
S43
設定メニュー一覧を表示
S42
その他の処理
S44
メニュー項目の選択操作？
Y
S45
選択中項目の変更表示
N
S46
項目決定操作？
N
Y
S47
選択された項目はドアロック制御モード設定？
N
S48
その他の項目の処理
Y
S49
オートロックモードと、逐次ロックモードとの選択画面表示
S50
オートロックモード選択？
Y
N
S52
逐次ロックモードを設定
S51
オートロックモードを設定
エンド

Fig.19

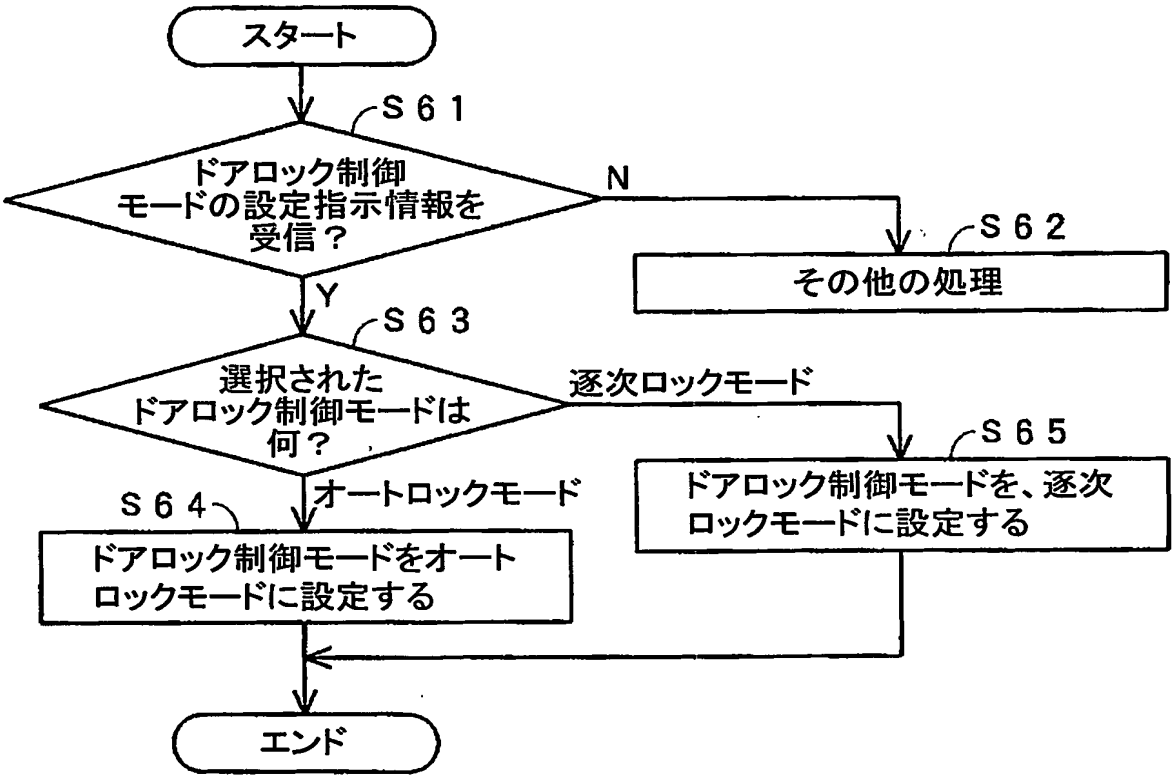

スタート
S61
ドアロック制御モードの設定指示情報を受信？
N
S62
その他の処理
Y
S63
選択されたドアロック制御モードは何？
逐次ロックモード
S65
ドアロック制御モードを、逐次ロックモードに設定する
オートロックモード
S64
ドアロック制御モードをオートロックモードに設定する
エンド

Fig.20

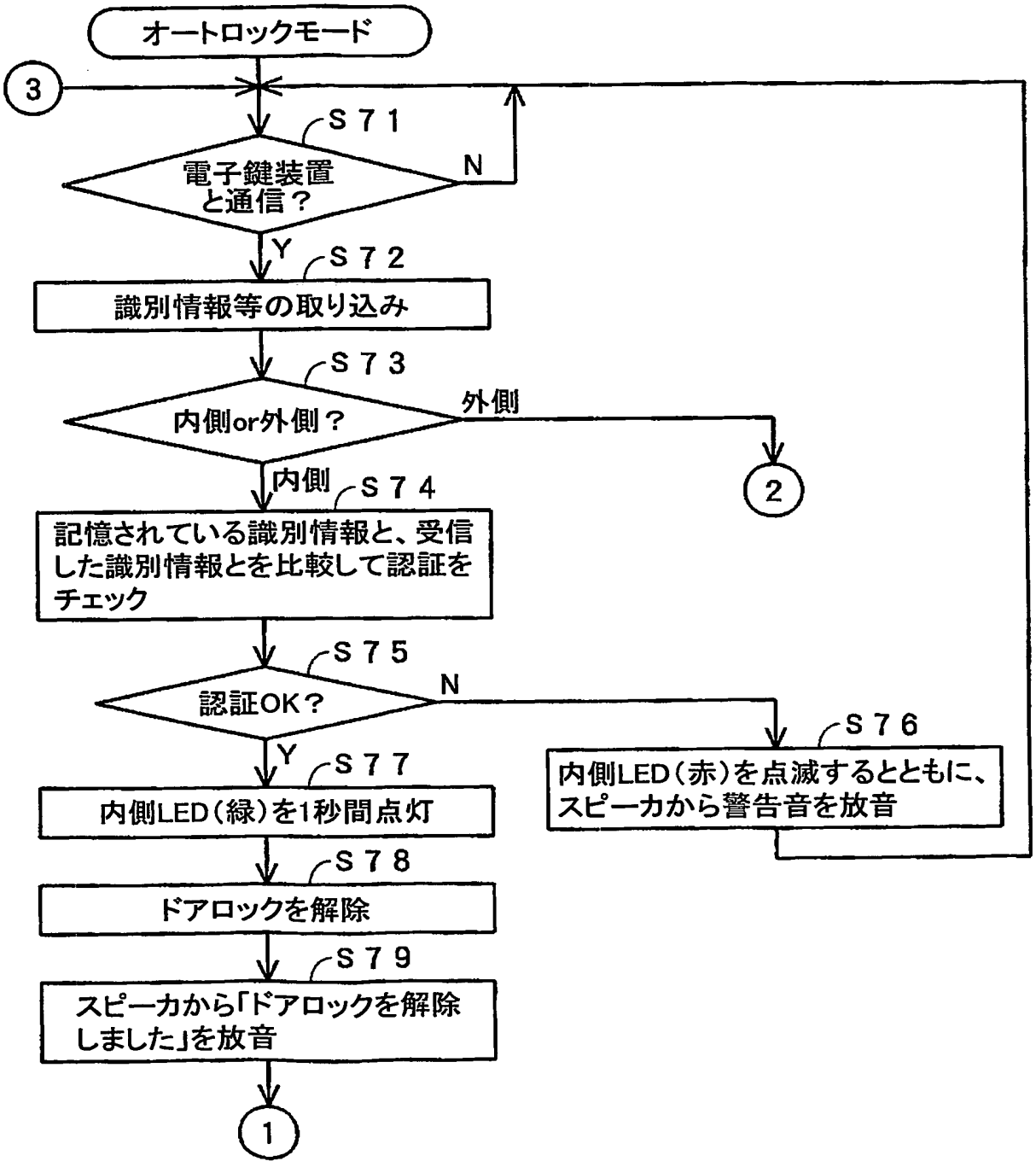

オートロックモード
3
S71
電子鍵装置と通信？
N
Y
S72
識別情報等の取り込み
S73
内側or外側？
外側
2
内側
S74
記憶されている識別情報と、受信した識別情報とを比較して認証をチェック
S75
認証OK？
N
S76
内側LED（赤）を点滅するとともに、スピーカから警告音を放音
Y
S77
内側LED（緑）を1秒間点灯
S78
ドアロックを解除
S79
スピーカから「ドアロックを解除しました」を放音
1

Fig.21

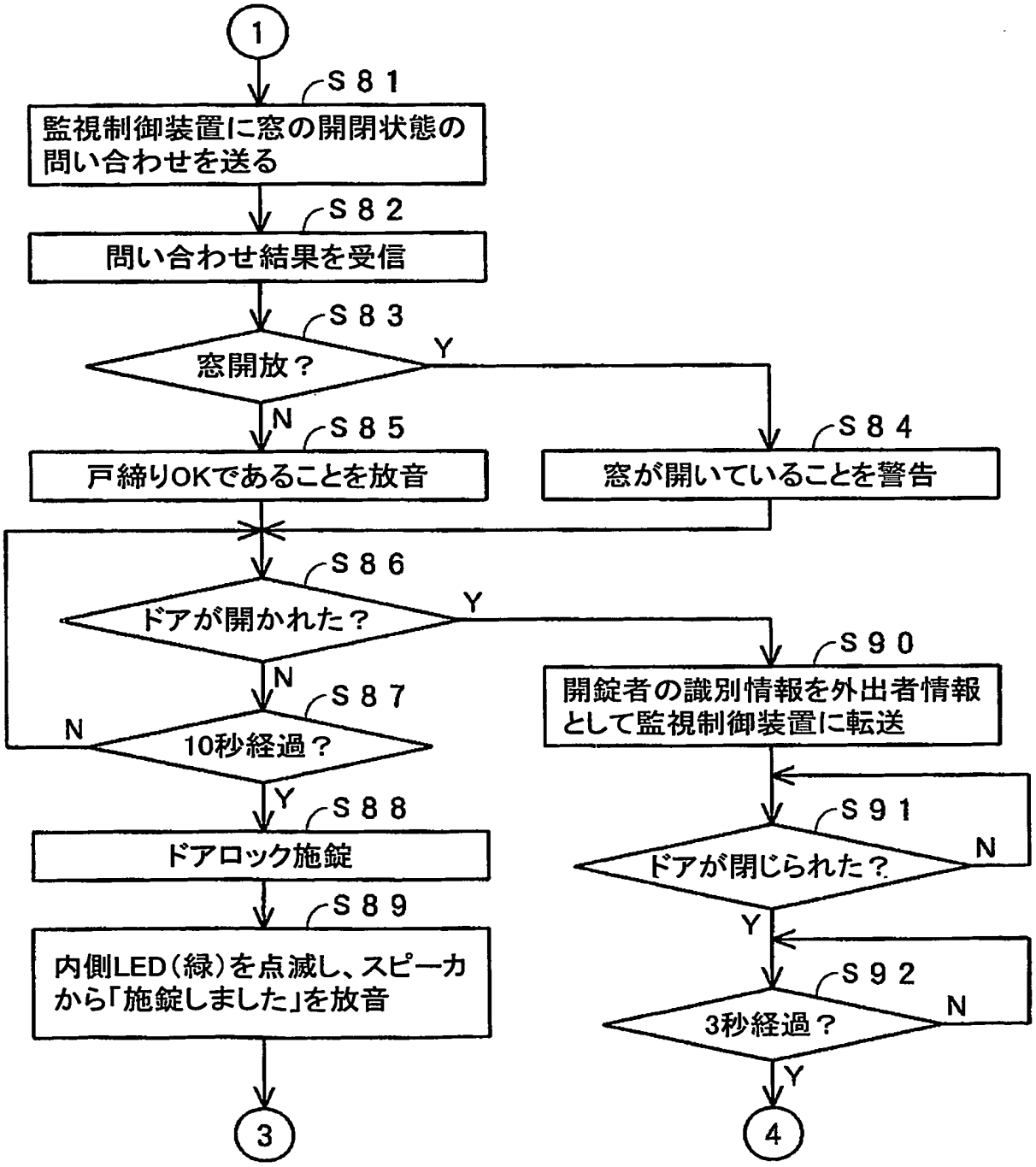

1
S81
監視制御装置に窓の開閉状態の問い合わせを送る
S82
問い合わせ結果を受信
S83
窓開放？
Y
N
S85
戸締りOKであることを放音
S84
窓が開いていることを警告
S86
ドアが開かれた？
Y
N
S87
10秒経過？
N
Y
S88
ドアロック施錠
S89
内側LED（緑）を点滅し、スピーカから「施錠しました」を放音
3
S90
開錠者の識別情報を外出者情報として監視制御装置に転送
S91
ドアが閉じられた？
N
Y
S92
3秒経過？
N
Y
4

Fig.22

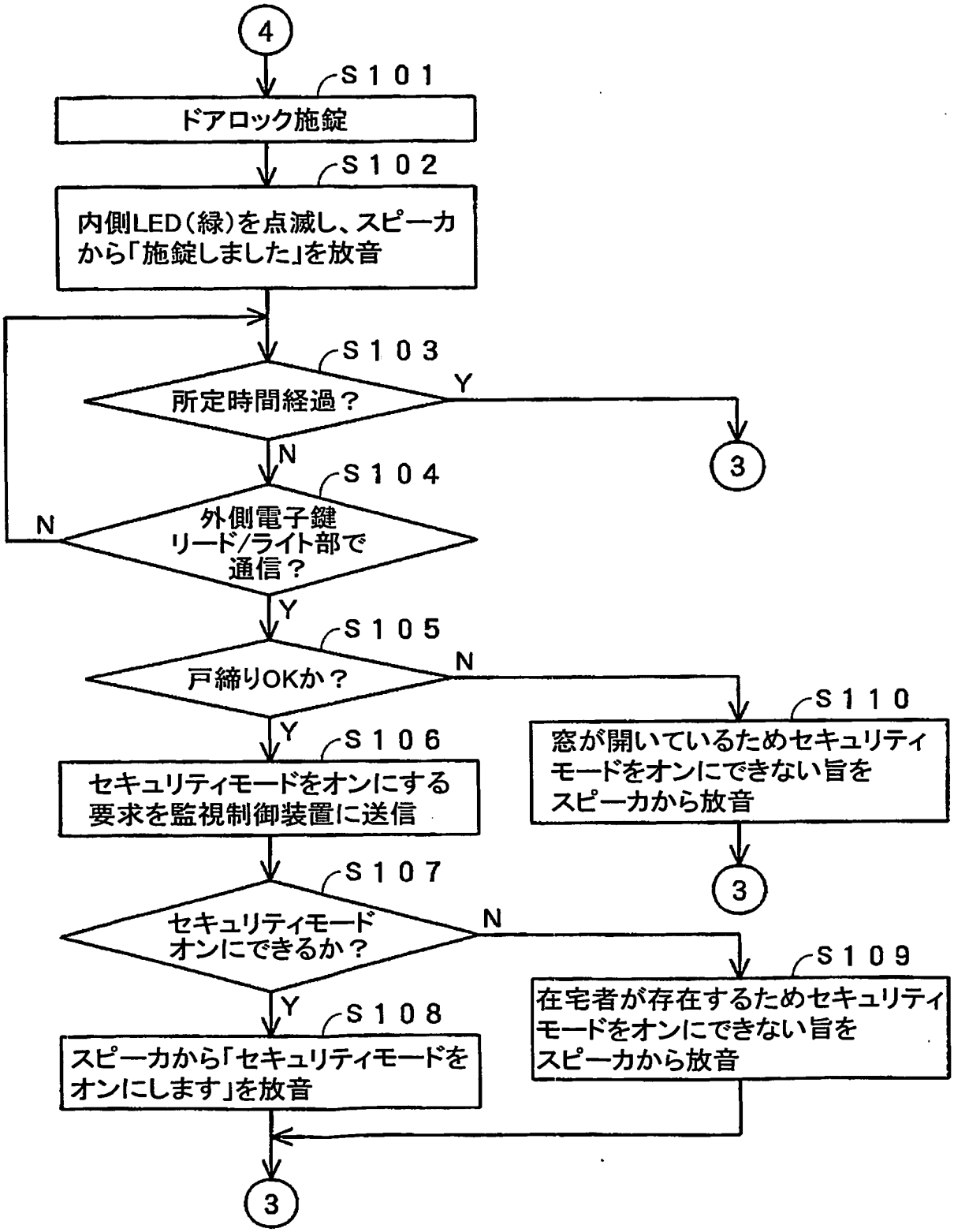

4
S101
ドアロック施錠
S102
内側LED(緑)を点滅し、スピーカから「施錠しました」を放音
S103
所定時間経過？
Y
N
3
S104
外側電子鍵リード/ライト部で通信？
N
Y
S105
戸締りOKか？
N
Y
S106
セキュリティモードをオンにする要求を監視制御装置に送信
S110
窓が開いているためセキュリティモードをオンにできない旨をスピーカから放音
3
S107
セキュリティモードオンにできるか？
N
Y
S108
スピーカから「セキュリティモードをオンにします」を放音
S109
在宅者が存在するためセキュリティモードをオンにできない旨をスピーカから放音
3

Fig.23

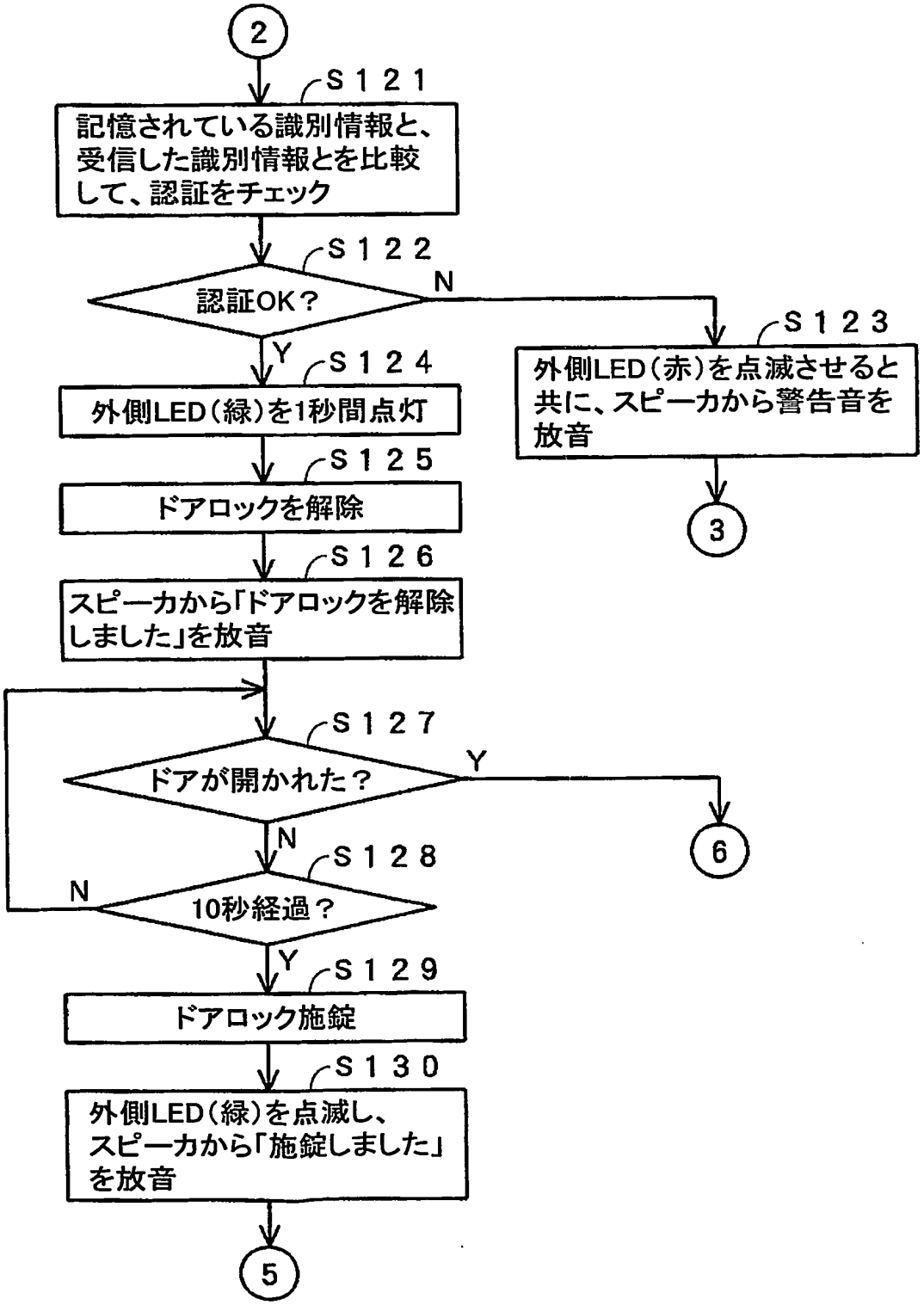

2
S121
記憶されている識別情報と、受信した識別情報とを比較して、認証をチェック
S122
認証OK？
N
Y
S123
外側LED（赤）を点滅させると共に、スピーカから警告音を放音
3
S124
外側LED（緑）を1秒間点灯
S125
ドアロックを解除
S126
スピーカから「ドアロックを解除しました」を放音
S127
ドアが開かれた？
Y
6
N
S128
10秒経過？
N
Y
S129
ドアロック施錠
S130
外側LED（緑）を点滅し、スピーカから「施錠しました」を放音
5

Fig.24

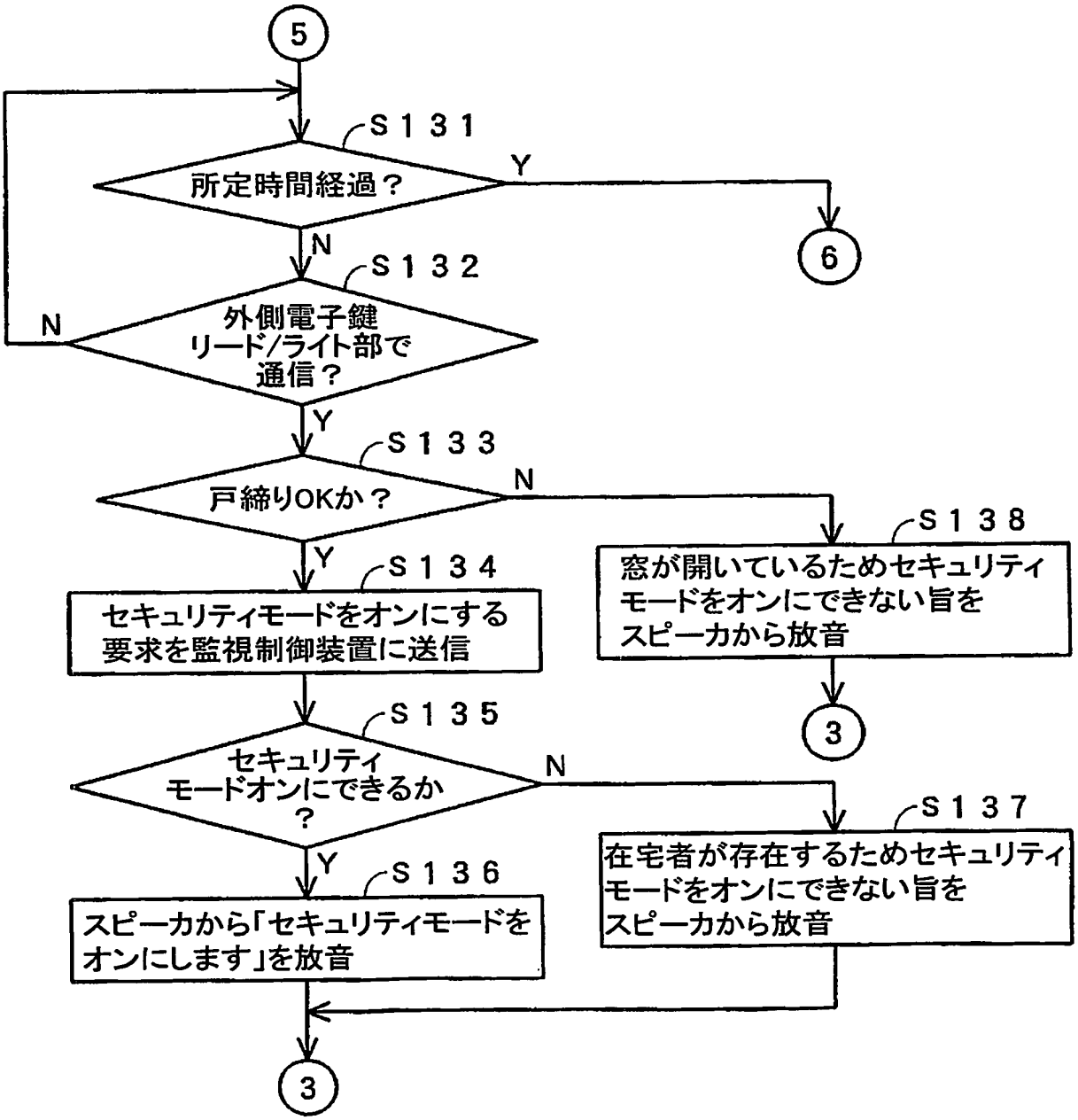

5
S131
所定時間経過？
Y
6
N
S132
外側電子鍵
リード/ライト部で
通信？
N
Y
S133
戸締りOKか？
N
S138
窓が開いているためセキュリティ
モードをオンにできない旨を
スピーカから放音
3
Y
S134
セキュリティモードをオンにする
要求を監視制御装置に送信
S135
セキュリティ
モードオンにできるか
？
N
S137
在宅者が存在するためセキュリティ
モードをオンにできない旨を
スピーカから放音
Y
S136
スピーカから「セキュリティモードを
オンにします」を放音
3

Fig.25

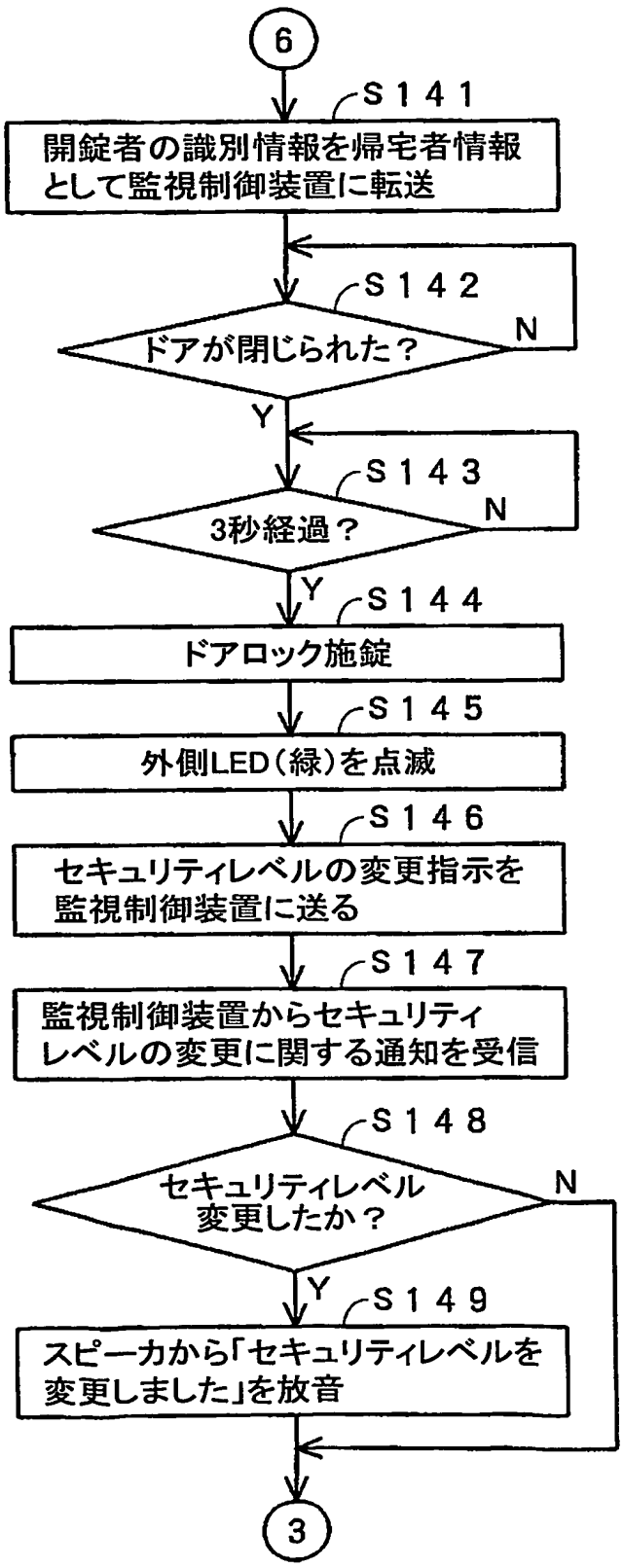

6
S141
開錠者の識別情報を帰宅者情報として監視制御装置に転送
S142
ドアが閉じられた？
N
Y
S143
3秒経過？
N
Y
S144
ドアロック施錠
S145
外側LED（緑）を点滅
S146
セキュリティレベルの変更指示を監視制御装置に送る
S147
監視制御装置からセキュリティレベルの変更に関する通知を受信
S148
セキュリティレベル変更したか？
N
Y
S149
スピーカから「セキュリティレベルを変更しました」を放音
3

Fig.26

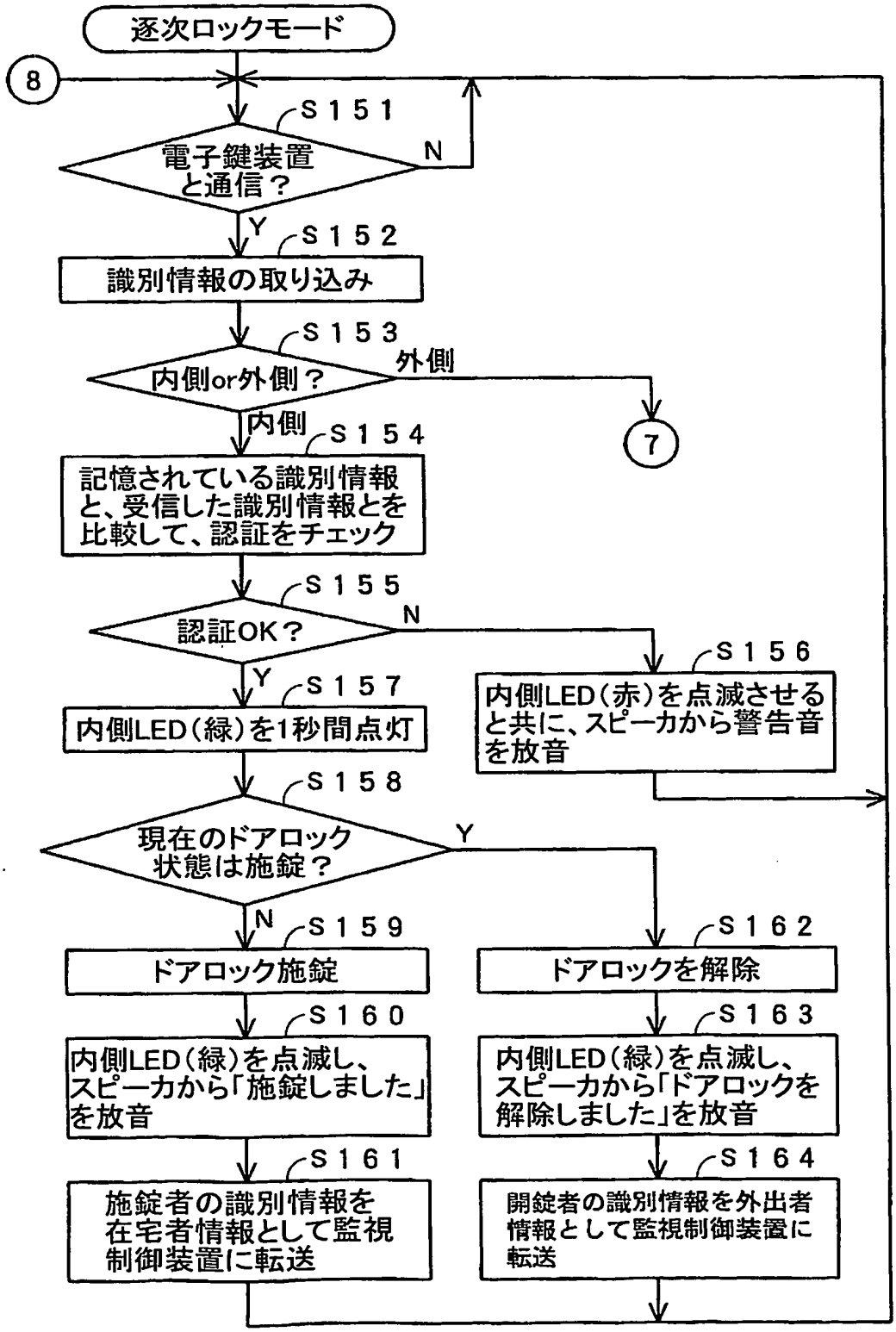

逐次ロックモード
8
S151
電子鍵装置と通信？
N
Y
S152
識別情報の取り込み
S153
内側or外側？
外側
7
内側
S154
記憶されている識別情報と、受信した識別情報とを比較して、認証をチェック
S155
認証OK？
N
S156
内側LED(赤)を点滅させると共に、スピーカから警告音を放音
Y
S157
内側LED(緑)を1秒間点灯
S158
現在のドアロック状態は施錠？
Y
N
S159
ドアロック施錠
S160
内側LED(緑)を点滅し、スピーカから「施錠しました」を放音
S161
施錠者の識別情報を在宅者情報として監視制御装置に転送
S162
ドアロックを解除
S163
内側LED(緑)を点滅し、スピーカから「ドアロックを解除しました」を放音
S164
開錠者の識別情報を外出者情報として監視制御装置に転送

Fig.27

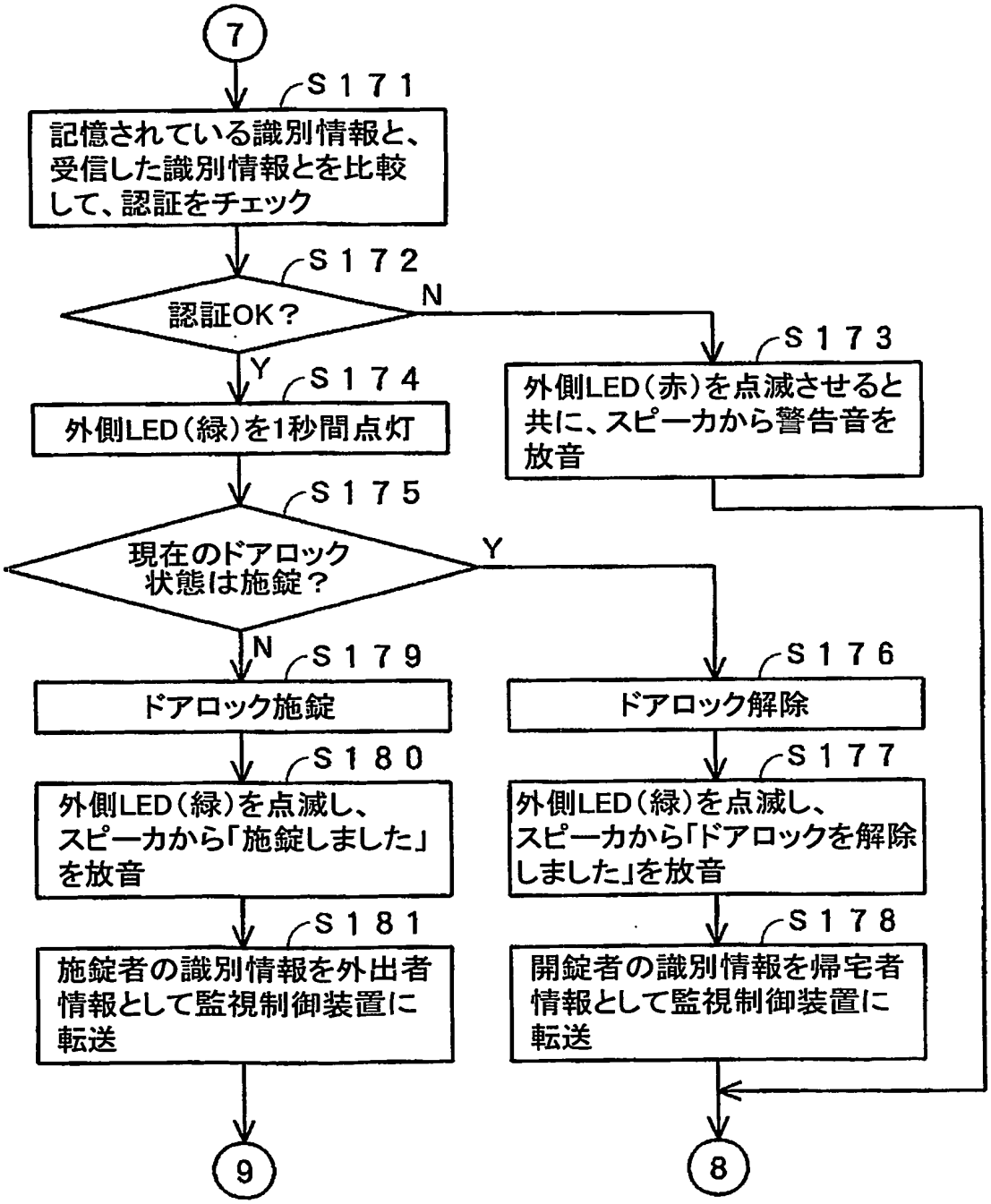

7
S171
記憶されている識別情報と、受信した識別情報とを比較して、認証をチェック
S172
認証OK？
N
Y
S173
外側LED（赤）を点滅させると共に、スピーカから警告音を放音
S174
外側LED（緑）を1秒間点灯
S175
現在のドアロック状態は施錠？
Y
N
S179
ドアロック施錠
S176
ドアロック解除
S180
外側LED（緑）を点滅し、スピーカから「施錠しました」を放音
S177
外側LED（緑）を点滅し、スピーカから「ドアロックを解除しました」を放音
S181
施錠者の識別情報を外出者情報として監視制御装置に転送
S178
開錠者の識別情報を帰宅者情報として監視制御装置に転送
9
8

Fig.28

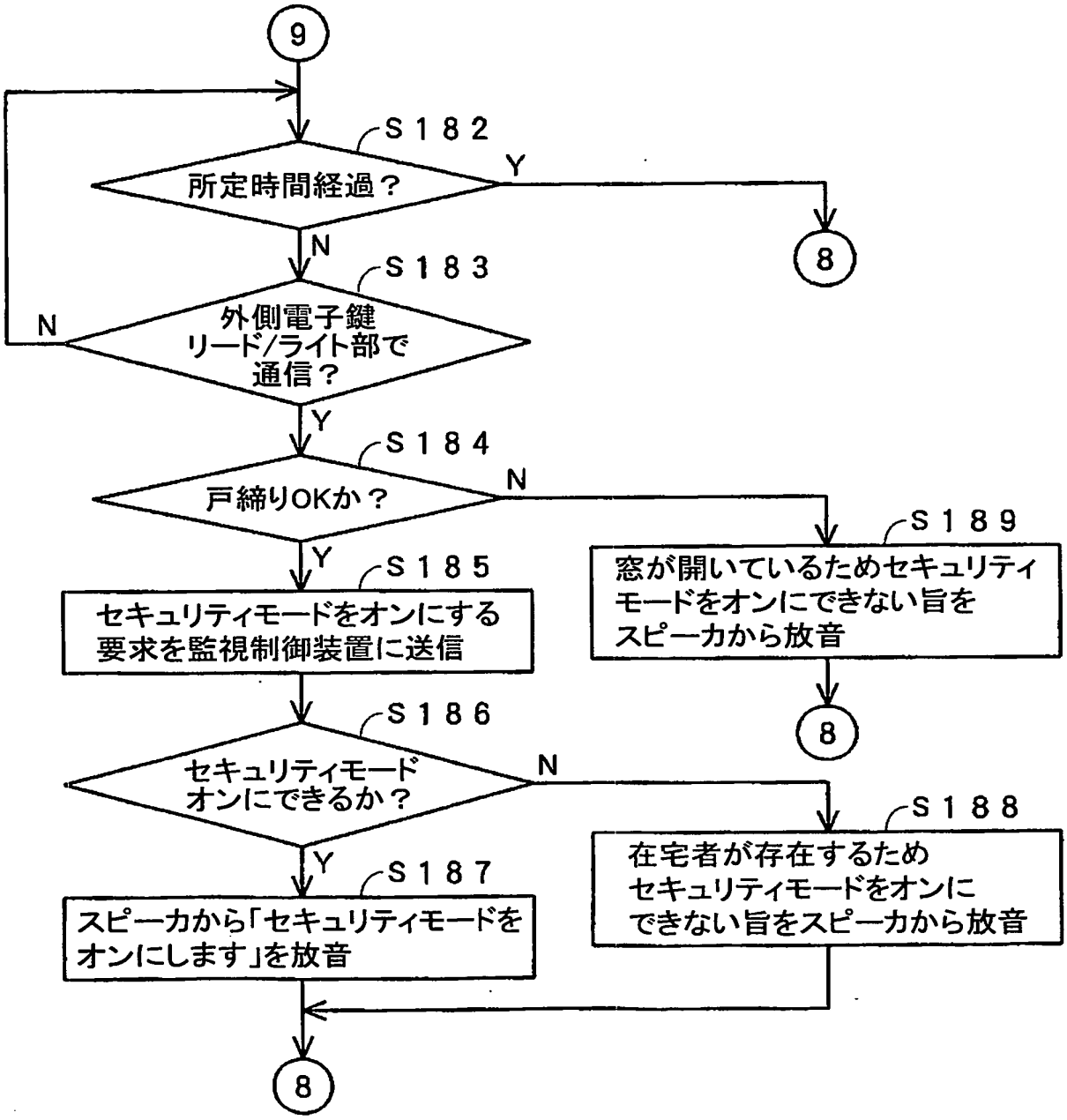

9
S182
所定時間経過？
Y
8
N
S183
外側電子鍵
リード/ライト部で
通信？
N
Y
S184
戸締りOKか？
N
S189
窓が開いているためセキュリティ
モードをオンにできない旨を
スピーカから放音
8
Y
S185
セキュリティモードをオンにする
要求を監視制御装置に送信
S186
セキュリティモード
オンにできるか？
N
S188
在宅者が存在するため
セキュリティモードをオンに
できない旨をスピーカから放音
Y
S187
スピーカから「セキュリティモードを
オンにします」を放音
8

Fig.29

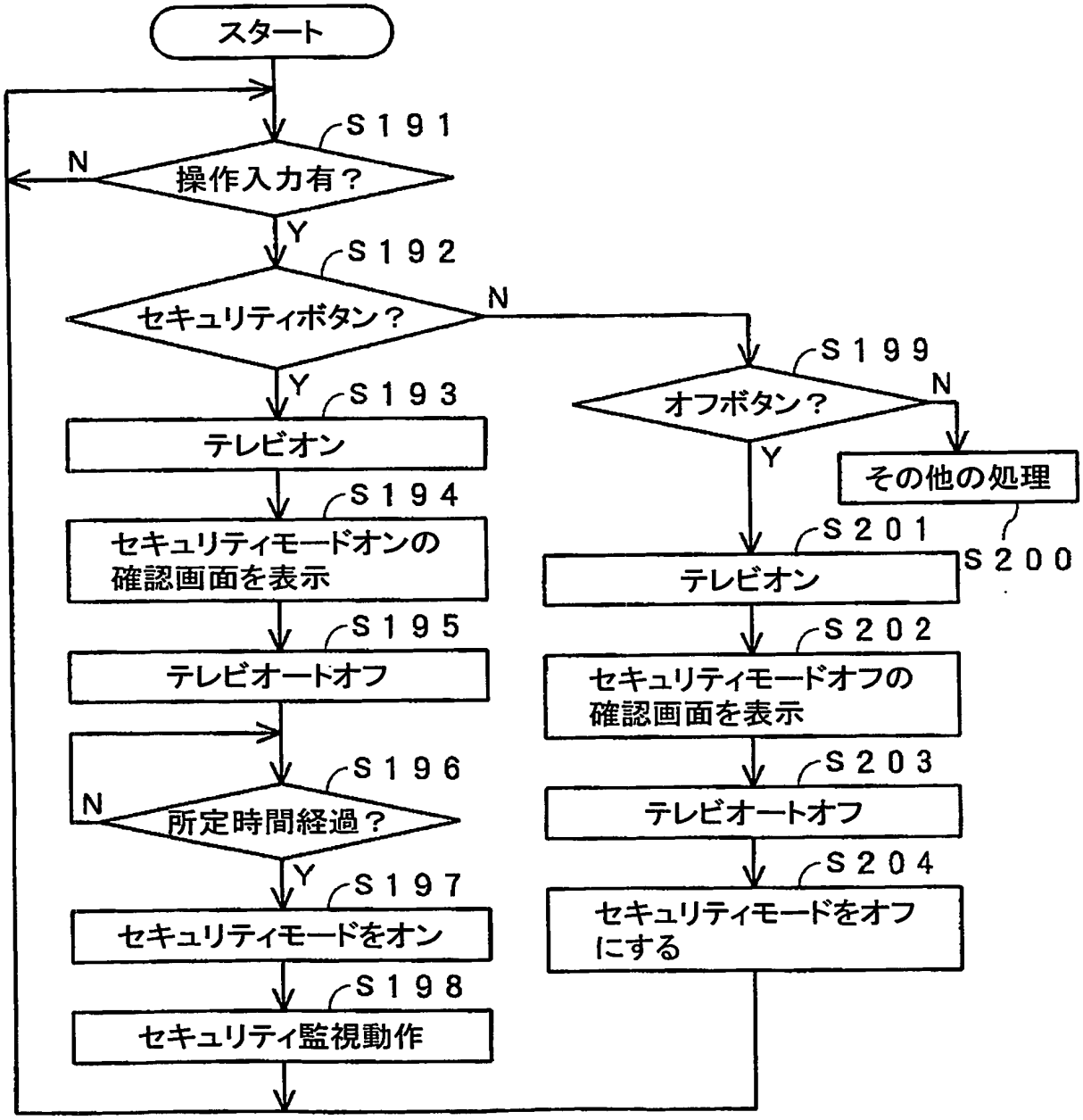

スタート
S191
操作入力有？
N
Y
S192
セキュリティボタン？
N
Y
S193
テレビオン
S194
セキュリティモードオンの
確認画面を表示
S195
テレビオートオフ
S196
所定時間経過？
N
Y
S197
セキュリティモードをオン
S198
セキュリティ監視動作
S199
オフボタン？
N
Y
その他の処理
S200
S201
テレビオン
S202
セキュリティモードオフの
確認画面を表示
S203
テレビオートオフ
S204
セキュリティモードをオフ
にする

Fig.30

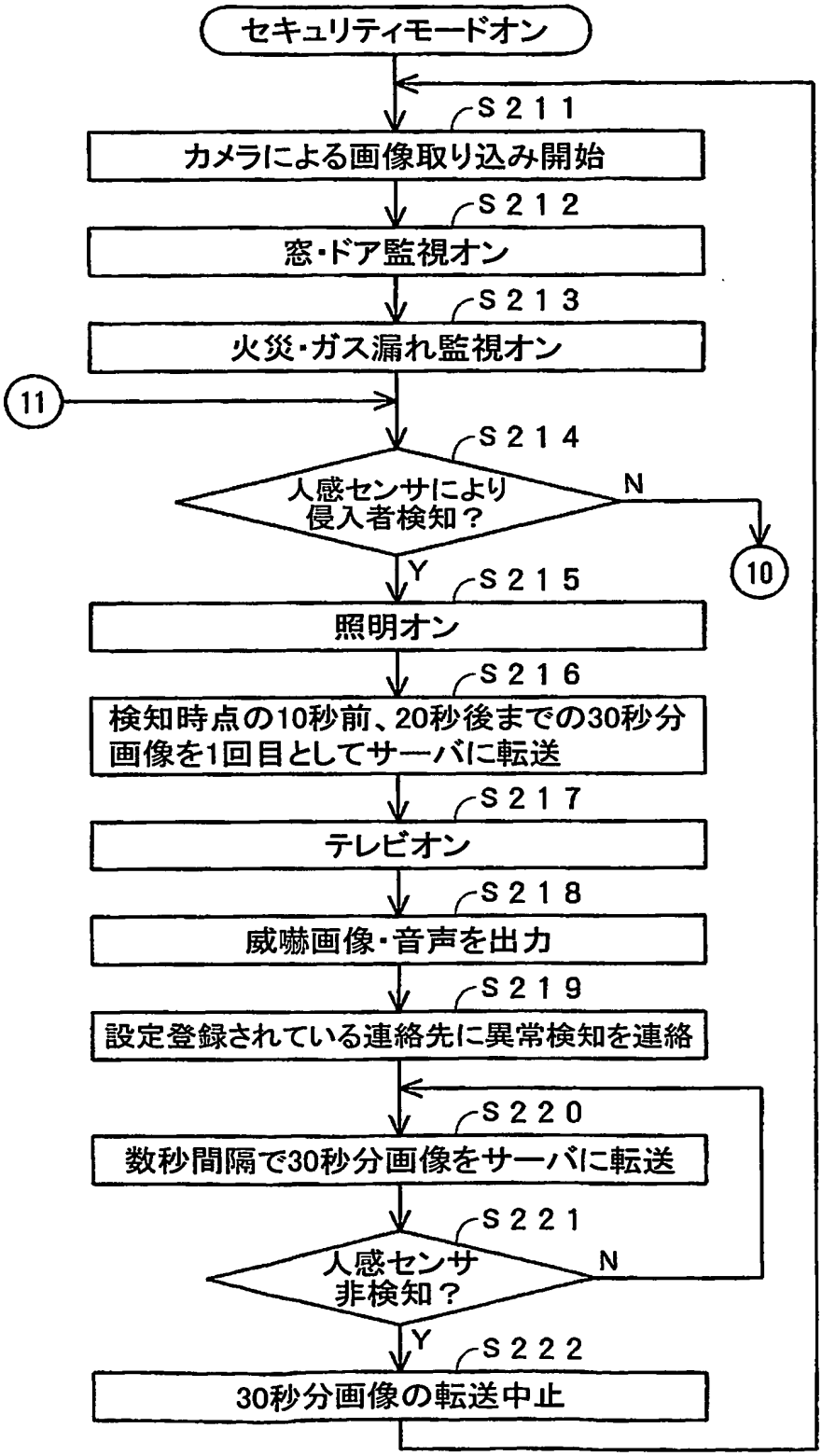

セキュリティモードオン
S211
カメラによる画像取り込み開始
S212
窓・ドア監視オン
S213
火災・ガス漏れ監視オン
11
S214
人感センサにより
侵入者検知？
N
10
Y
S215
照明オン
S216
検知時点の10秒前、20秒後までの30秒分
画像を1回目としてサーバに転送
S217
テレビオン
S218
威嚇画像・音声を出力
S219
設定登録されている連絡先に異常検知を連絡
S220
数秒間隔で30秒分画像をサーバに転送
S221
人感センサ
非検知？
N
Y
S222
30秒分画像の転送中止

Fig.31

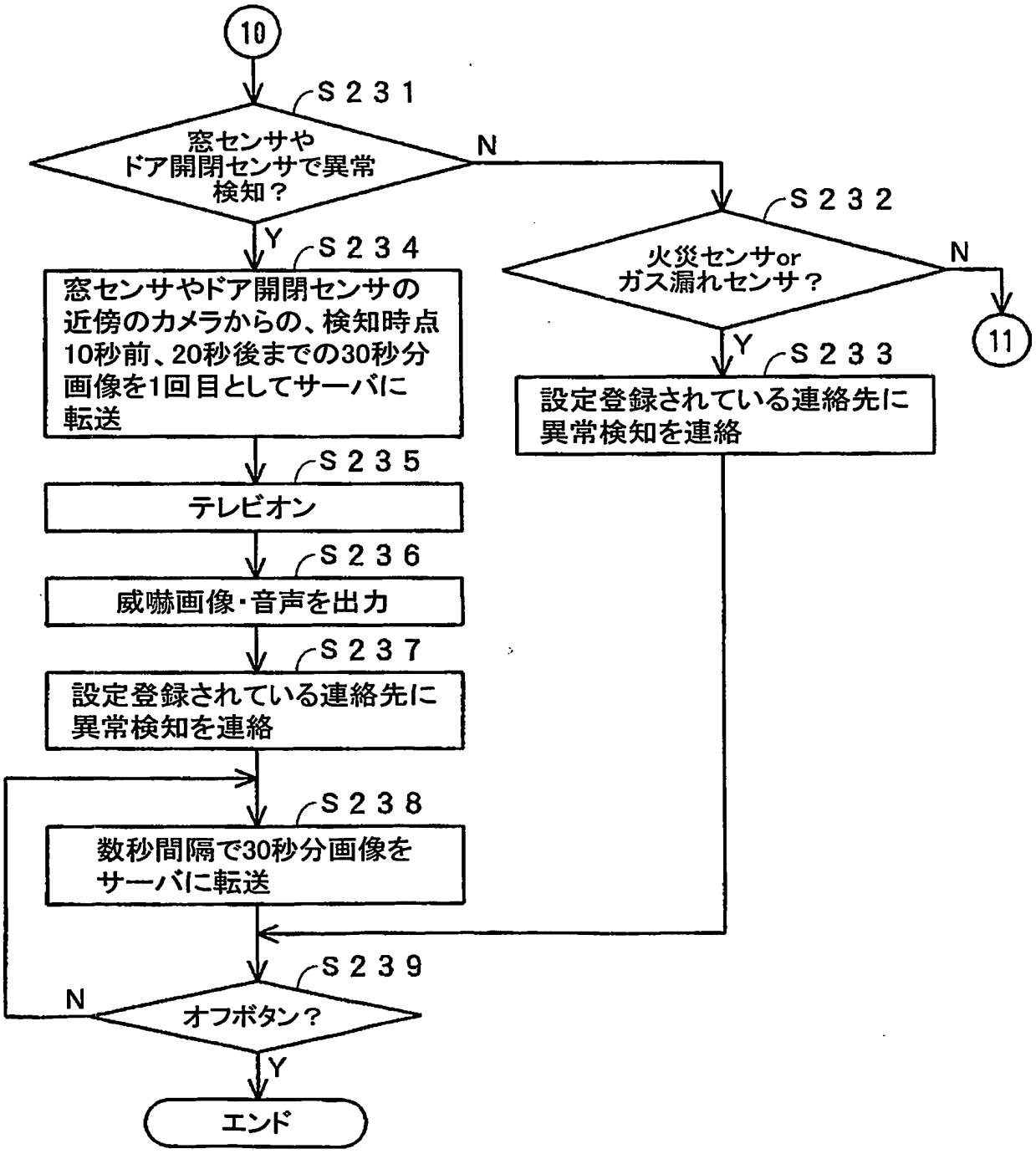

10
S231
窓センサや
ドア開閉センサで異常
検知？
N
Y
S232
火災センサor
ガス漏れセンサ？
N
11
Y
S233
設定登録されている連絡先に
異常検知を連絡
S234
窓センサやドア開閉センサの
近傍のカメラからの、検知時点
10秒前、20秒後までの30秒分
画像を1回目としてサーバに
転送
S235
テレビオン
S236
威嚇画像・音声を出力
S237
設定登録されている連絡先に
異常検知を連絡
S238
数秒間隔で30秒分画像を
サーバに転送
S239
N
オフボタン？
Y
エンド

Fig.32

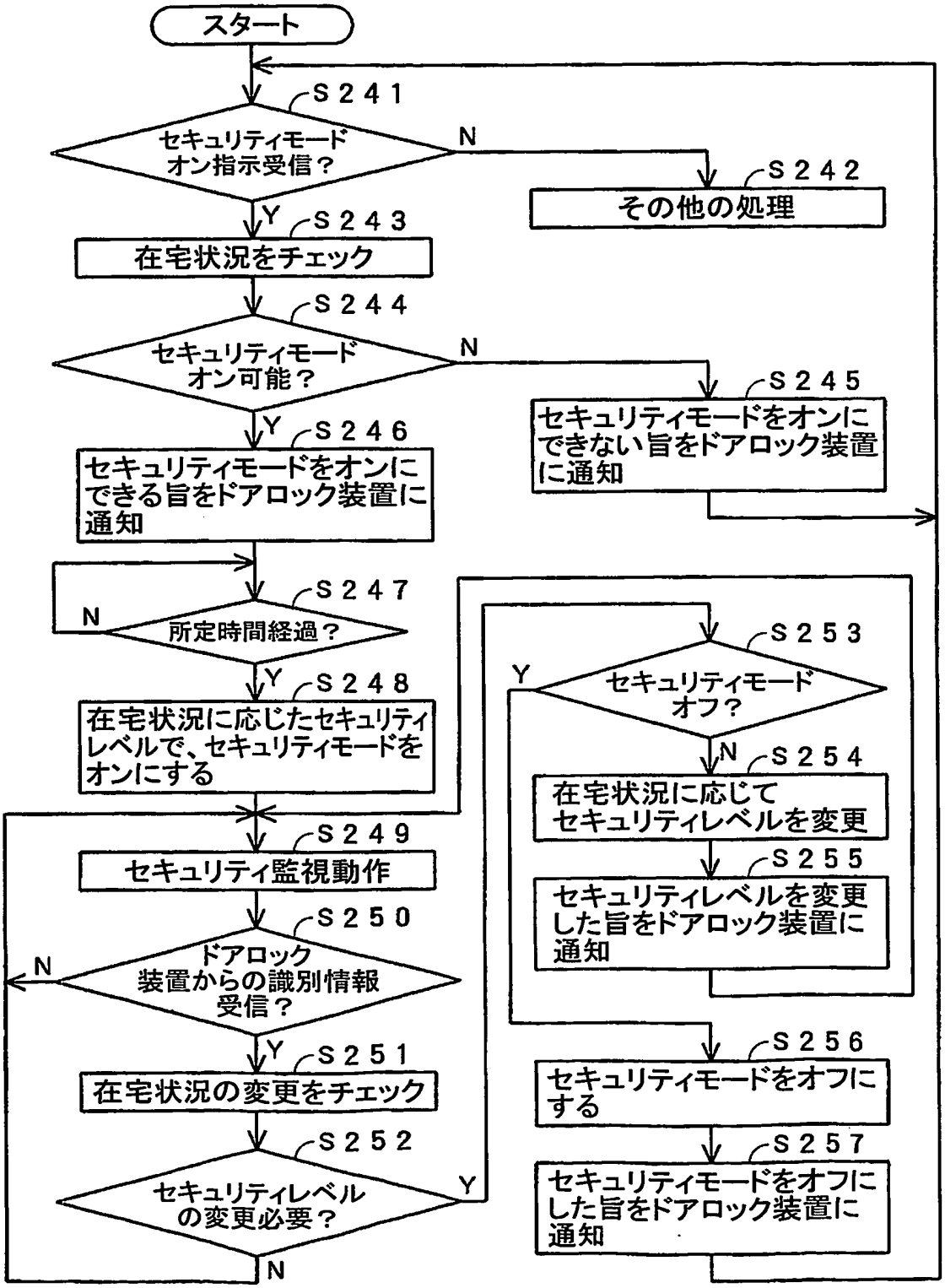

スタート
S241
セキュリティモード
オン指示受信？
N
S242
その他の処理
Y
S243
在宅状況をチェック
S244
セキュリティモード
オン可能？
N
S245
セキュリティモードをオンに
できない旨をドアロック装置
に通知
Y
S246
セキュリティモードをオンに
できる旨をドアロック装置に
通知
S247
N
所定時間経過？
Y
S248
在宅状況に応じたセキュリティ
レベルで、セキュリティモードを
オンにする
S249
セキュリティ監視動作
S250
N
ドアロック
装置からの識別情報
受信？
Y
S251
在宅状況の変更をチェック
S252
セキュリティレベル
の変更必要？
Y
N
S253
Y
セキュリティモード
オフ？
N
S254
在宅状況に応じて
セキュリティレベルを変更
S255
セキュリティレベルを変更
した旨をドアロック装置に
通知
S256
セキュリティモードをオフに
する
S257
セキュリティモードをオフに
した旨をドアロック装置に
通知

Fig.33

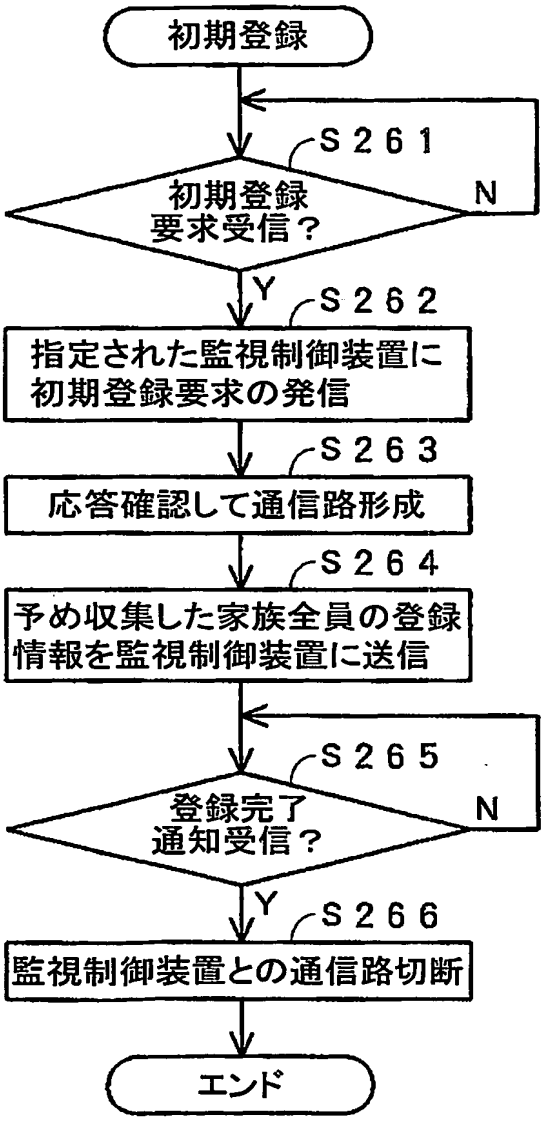

初期登録
S261
初期登録
要求受信？
N
Y
S262
指定された監視制御装置に
初期登録要求の発信
S263
応答確認して通信路形成
S264
予め収集した家族全員の登録
情報を監視制御装置に送信
S265
登録完了
通知受信？
N
Y
S266
監視制御装置との通信路切断
エンド

Fig.34

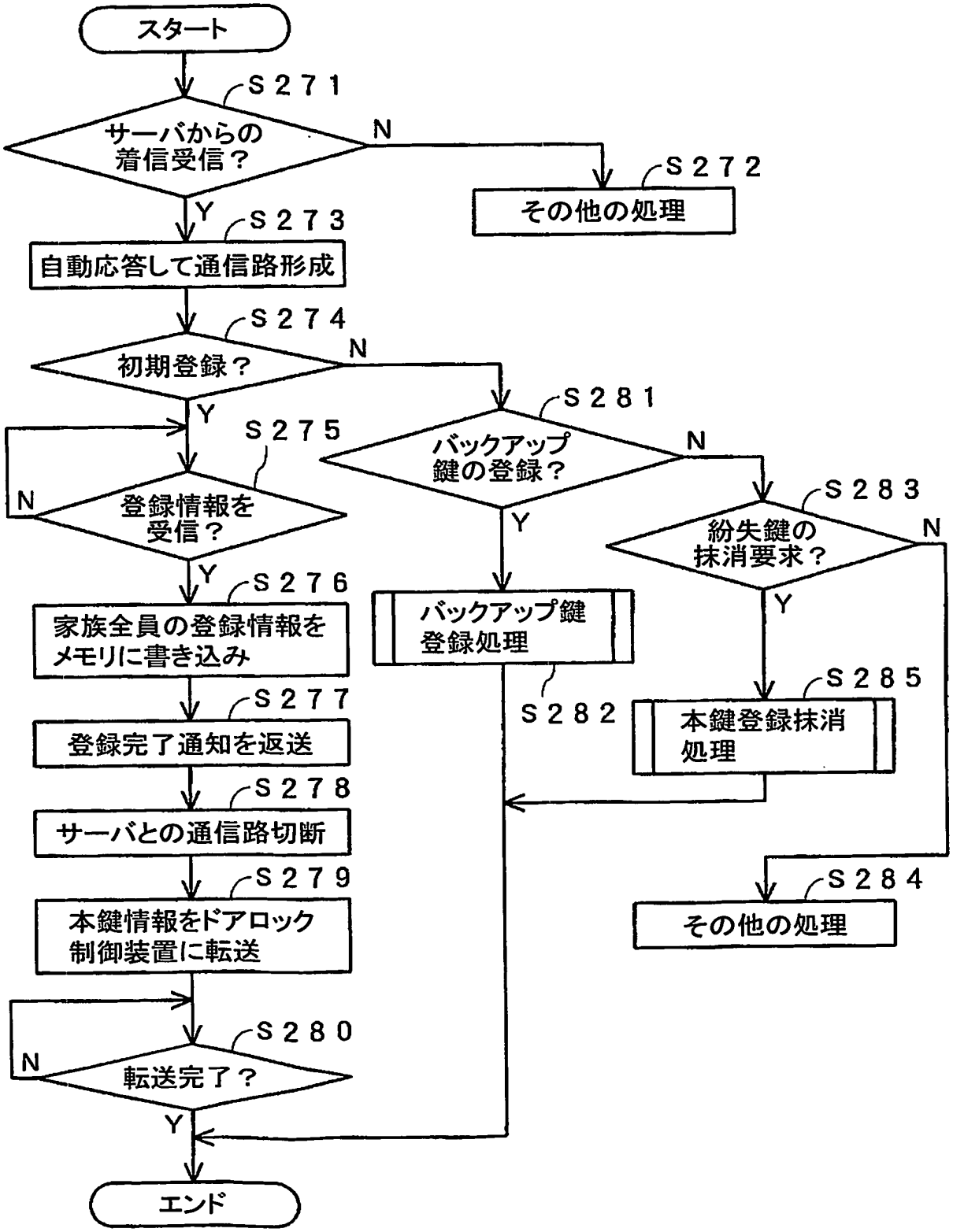

スタート
S271
サーバからの着信受信？
N
S272
その他の処理
Y
S273
自動応答して通信路形成
S274
初期登録？
N
Y
S275
登録情報を受信？
N
Y
S276
家族全員の登録情報をメモリに書き込み
S277
登録完了通知を返送
S278
サーバとの通信路切断
S279
本鍵情報をドアロック制御装置に転送
S280
転送完了？
N
Y
エンド
S281
バックアップ鍵の登録？
N
Y
バックアップ鍵登録処理
S282
S283
紛失鍵の抹消要求？
N
Y
S285
本鍵登録抹消処理
S284
その他の処理

Fig.35

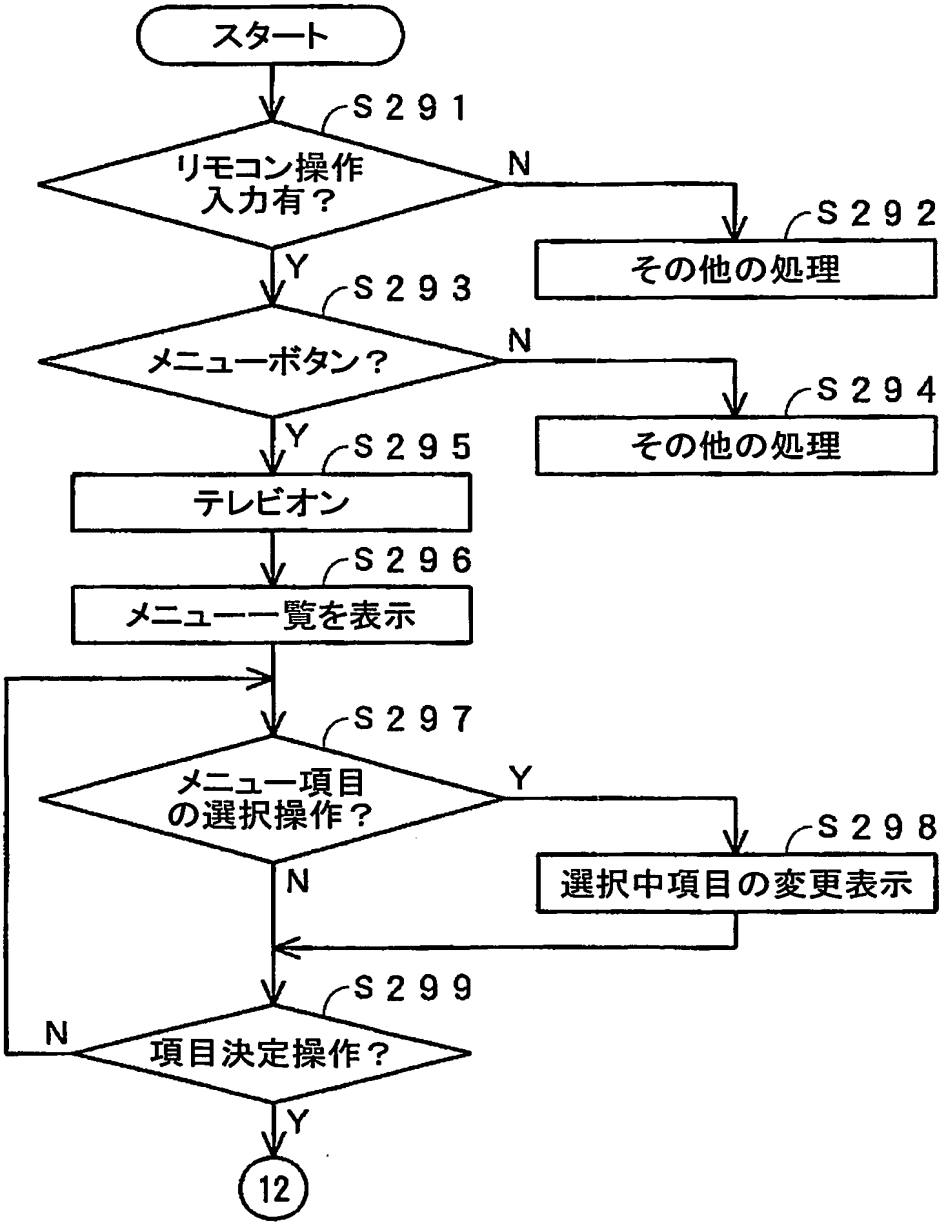

スタート
S291
リモコン操作入力有？
N
S292
その他の処理
Y
S293
メニューボタン？
N
S294
その他の処理
Y
S295
テレビオン
S296
メニュー一覧を表示
S297
メニュー項目の選択操作？
Y
S298
選択中項目の変更表示
N
S299
N
項目決定操作？
Y
12

Fig.36

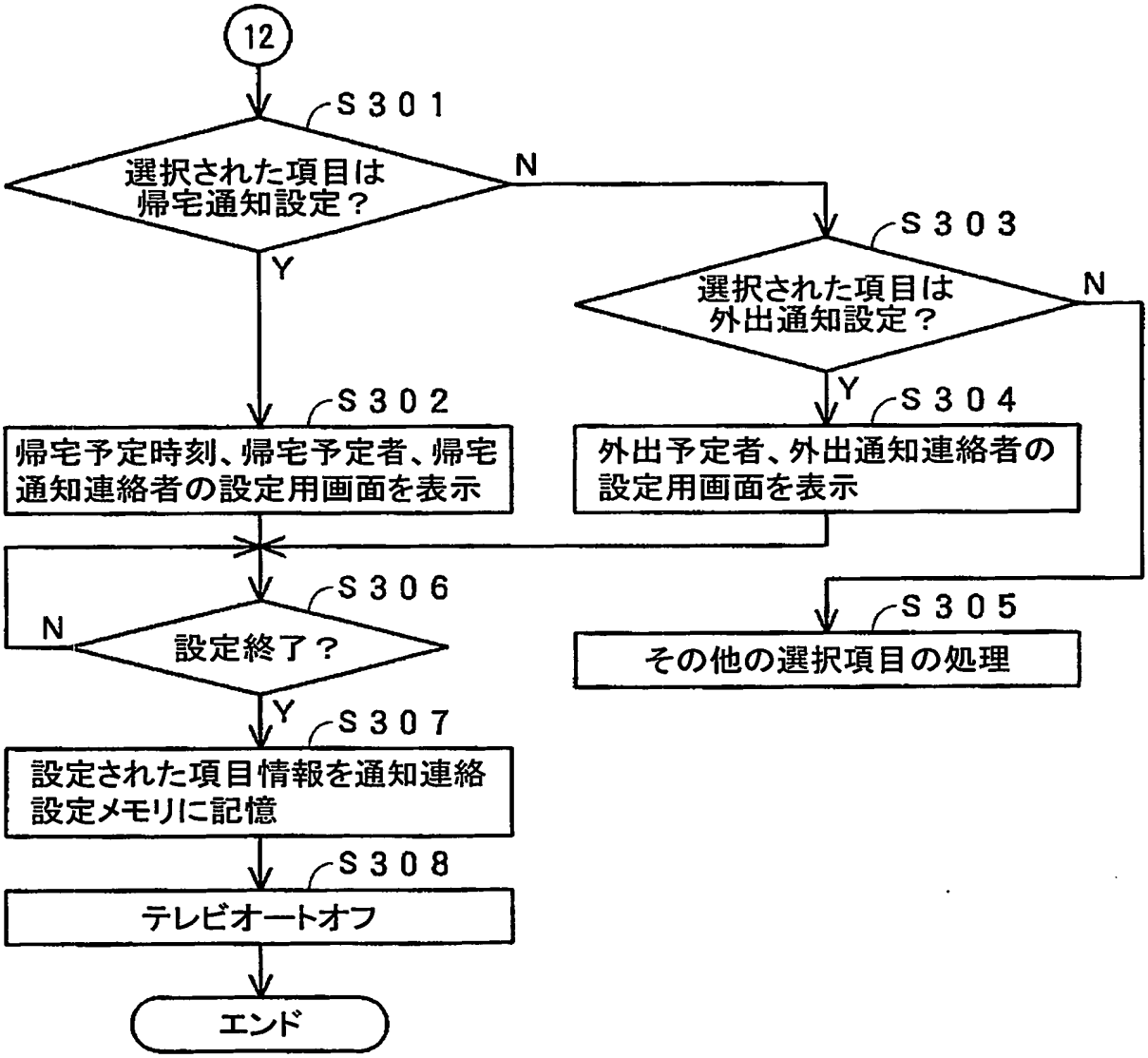

12
S301
選択された項目は帰宅通知設定？
N
Y
S303
選択された項目は外出通知設定？
N
Y
S302
帰宅予定時刻、帰宅予定者、帰宅通知連絡者の設定用画面を表示
S304
外出予定者、外出通知連絡者の設定用画面を表示
S306
N
設定終了？
S305
その他の選択項目の処理
Y
S307
設定された項目情報を通知連絡設定メモリに記憶
S308
テレビオートオフ
エンド

Fig.37

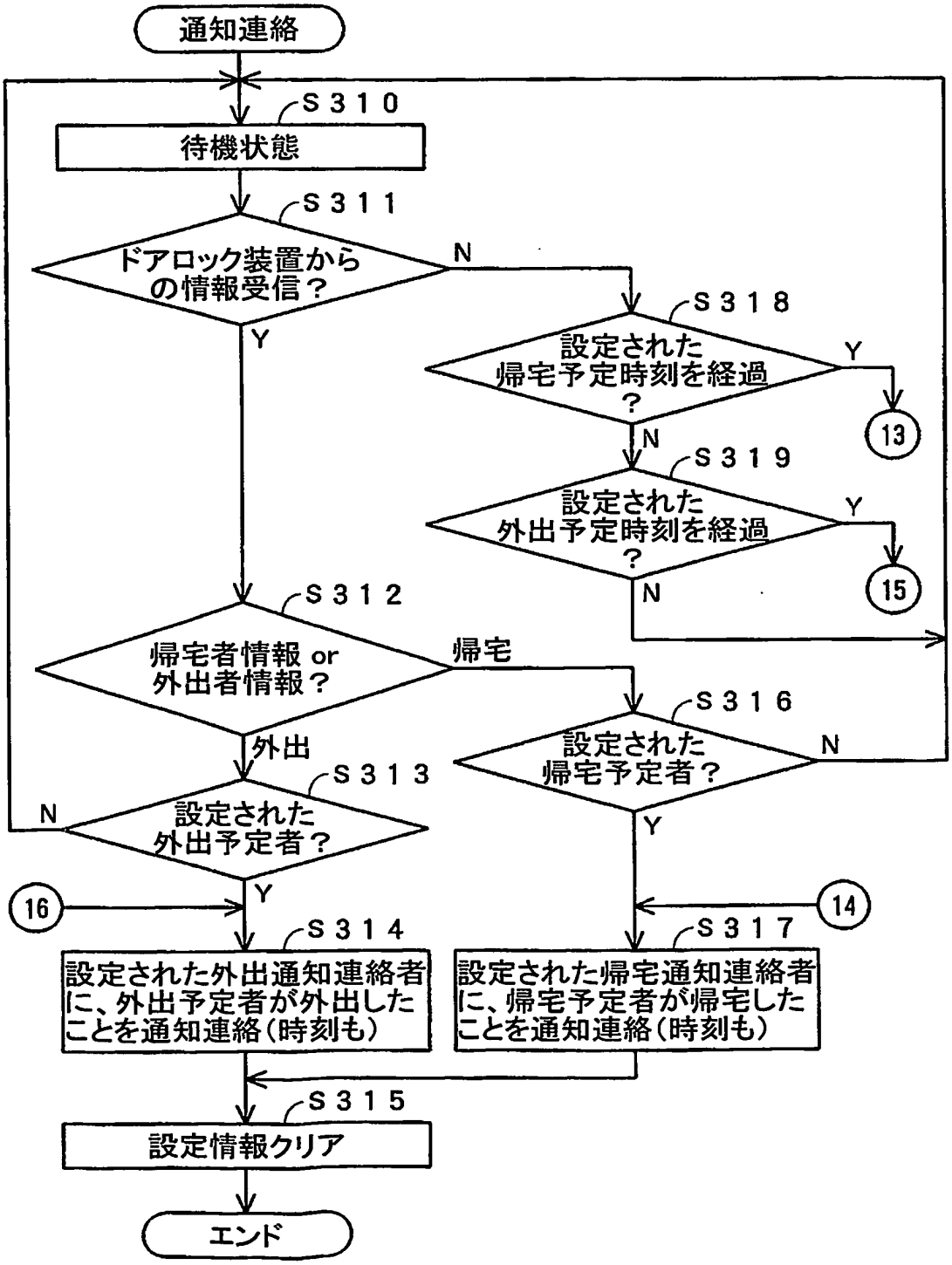

通知連絡
S310
待機状態
S311
ドアロック装置からの情報受信？
N
Y
S318
設定された帰宅予定時刻を経過？
Y
13
N
S319
設定された外出予定時刻を経過？
Y
15
N
S312
帰宅者情報 or 外出者情報？
帰宅
外出
S316
設定された帰宅予定者？
N
Y
S313
設定された外出予定者？
N
Y
16
14
S314
設定された外出通知連絡者に、外出予定者が外出したことを通知連絡（時刻も）
S317
設定された帰宅通知連絡者に、帰宅予定者が帰宅したことを通知連絡（時刻も）
S315
設定情報クリア
エンド

Fig.38

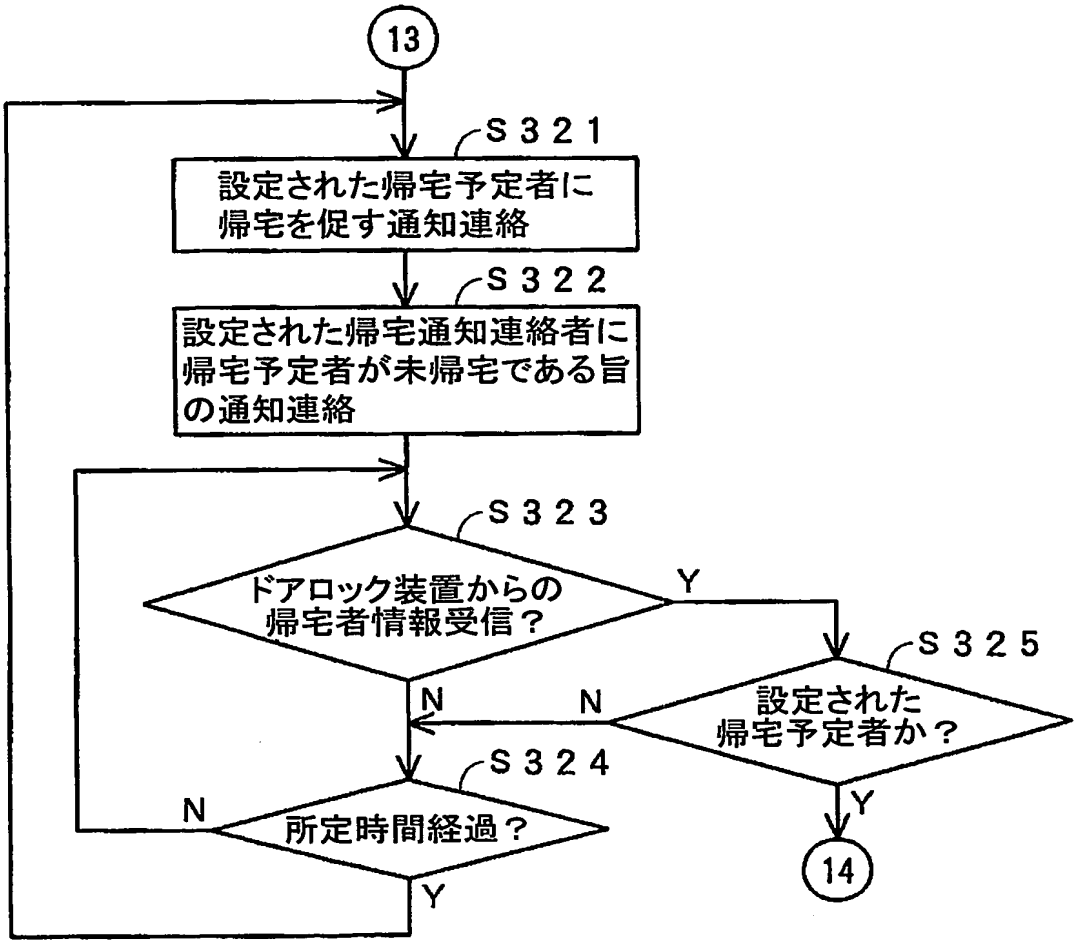

13
S321
設定された帰宅予定者に帰宅を促す通知連絡
S322
設定された帰宅通知連絡者に帰宅予定者が未帰宅である旨の通知連絡
S323
ドアロック装置からの帰宅者情報受信？
Y
N
S325
設定された帰宅予定者か？
N
Y
S324
所定時間経過？
N
Y
14

Fig.39

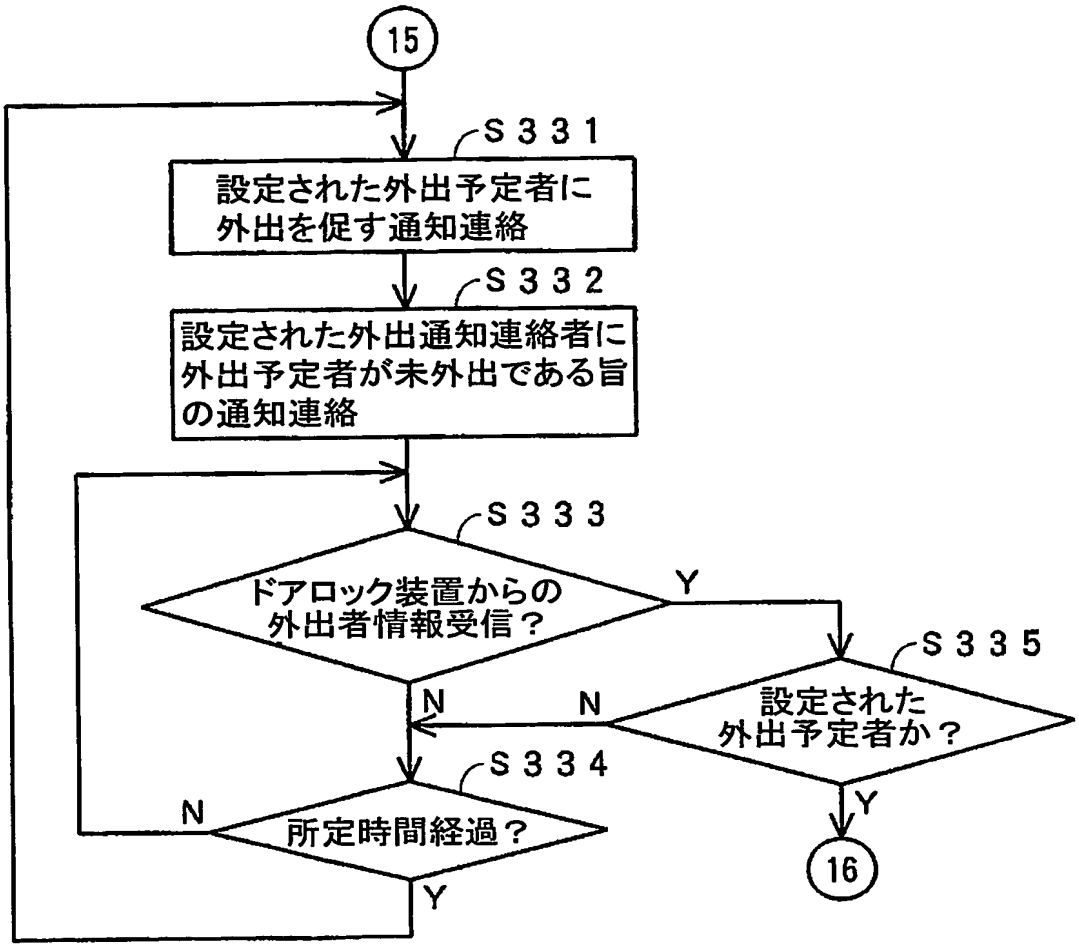

15
S 3 3 1
設定された外出予定者に
外出を促す通知連絡
S 3 3 2
設定された外出通知連絡者に
外出予定者が未外出である旨
の通知連絡
S 3 3 3
ドアロック装置からの
外出者情報受信？
Y
S 3 3 5
設定された
外出予定者か？
N
N
S 3 3 4
所定時間経過？
N
Y
Y
16

Fig.40

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/JP03/09755

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] E05B49/00, G08B25/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] E05B49/00-49/04, G08B23/00-31/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Toroku Jitsuyo Shinan Koho	1994-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2002-70377 A (Yokogawa Electric Corp.), 08 March, 2002 (08.03.02), Full text; all drawings (Family: none)	1,7 2-6,8
Y	JP 2002-16714 A (Matsushita Electric Works, Ltd.), 18 January, 2002 (18.01.02), Full text; all drawings (Family: none)	2-6,8
Y	JP 2000-259971 A (Kabushiki Kaisha Shin Shakai Shihon Joho Kaihatsu Center), 22 September, 2000 (22.09.00), Full text; all drawings (Family: none)	3-6

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 05 September, 2003 (05.09.03)	Date of mailing of the international search report 07 October, 2003 (07.10.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/JP03/09755

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-268273 A (Aichi Tokei Denki Kabushiki Kaisha), 29 September, 2000 (29.09.00), Par. No. [0004] (Family: none)	3
Y	JP 11-45392 A (Matsushita Electric Works, Ltd.), 16 February, 1999 (16.02.99), Par. No. [0012] (Family: none)	3
Y	JP 2002-71478 A (Hitachi Government & Public Corporation System Engineering, Ltd.), 08 March, 2002 (08.03.02), Par. Nos. [0008] to [0010]; Fig. 1 (Family: none)	4

国際調査報[redacted]　　国際出願番号　P[redacted]／ＪＰ０３／０９７５５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｅ０５Ｂ４９／００，Ｇ０８Ｂ２５／０４

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｅ０５Ｂ４９／００－４９／０４，Ｇ０８Ｂ２３／００－３１／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００３年
日本国実用新案登録公報	１９９６－２００３年
日本国登録実用新案公報	１９９４－２００３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ　２００２－７０３７７　Ａ　（横河電機株式会社） ２００２．０３．０８，全文，全図（ファミリーなし）	１，７
Ｙ		２－６，８
Ｙ	ＪＰ　２００２－１６７１４　Ａ　（松下電工株式会社） ２００２．０１．１８，全文，全図（ファミリーなし）	２－６，８

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０５．０９．０３	国際調査報告の発送日 07.10.03
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 清藤　弘晃　２Ｒ　２９１６ 電話番号　０３－３５８１－１１０１　内線　３４２２

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　２０００－２５９７１　Ａ　（株式会社新社会資本情報開発センター）　２０００．０９．２２，全文，全図（ファミリーなし）	３－６
Ｙ	ＪＰ　２０００－２６８２７３　Ａ　（愛知時計電機株式会社）　２０００．０９．２９，【０００４】（ファミリーなし）	３
Ｙ	ＪＰ　１１－４５３９２　Ａ　（松下電工株式会社）　１９９９．０２．１６，【００１２】（ファミリーなし）	３
Ｙ	ＪＰ　２００２－７１３７８　Ａ　（日立公共システムエンジニアリング株式会社）　２００２．０３．０８，【０００８】－【００１０】，図１（ファミリーなし）	４